

**ELECTRONIC BOOK SECURITY  
AND COPYRIGHT PROTECTION SYSTEM**

**Related Applications**

This application is a continuation-in-part of U.S. Application Serial No. 07/991,074 entitled TELEVISION PROGRAM PACKAGING AND DELIVERY SYSTEM WITH MENU DRIVEN SUBSCRIBER ACCESS, filed December 9, 1992, and U.S. Application Serial No. 08/336,247 entitled ELECTRONIC BOOK SELECTION AND DELIVERY SYSTEM, filed November 7, 1994, and U.S. Application Serial No. 08/160,194 and PCT/ US93/11606 entitled ADVANCED SET-TOP TERMINAL FOR CABLE TELEVISION DELIVERY SYSTEMS, filed December 2, 1993, and U.S. Application Serial No. 08/906,469 entitled REPROGRAMMABLE TERMINAL FOR SUGGESTING PROGRAMS OFFERED ON A TELEVISION PROGRAM DELIVERY SYSTEM, filed August 5, 1997, and U.S. Application Serial No. 09/191,520 entitled DIGITAL BROADCAST PROGRAM ORDERING, filed November 13, 1998. These applications are incorporated by reference herein. Also incorporated by reference are co-pending U.S. Application Serial No. 09/237,827 entitled ELECTRONIC BOOK HAVING LIBRARY CATALOG MENU AND SEARCHING FEATURES, filed January 27, 1999, U.S. Application Serial No. 09/237,828 entitled ELECTRONIC BOOK ELECTRONIC LINKS, filed January 27, 1999, U.S. Application Serial No. 09/289,956, entitled ELECTRONIC BOOK ALTERNATIVE DELIVERY METHODS, filed on April 13, 1999, and U.S. Application Serial No. 09/289,957, entitled ELECTRONIC BOOK ALTERNATIVE DELIVERY SYSTEMS, filed on April 13, 1999.

**Background Art**

Sparked by the concept of an information superhighway, a revolution will take place in the distribution of books. Not since the introduction of Gutenberg's movable typeset printing has the world stood on the brink of such a revolution in the distribution of text material. The definition of the word book will change drastically in the near future. Due to reasons such as security, convenience, cost, and other technical problems,

1 book and magazine publishers are currently only able to distribute their products in paper  
2 form. This invention solves the problems encountered by publishers.

3 Technical Field And Brief Summary Of Invention

4 The electronic book selection and delivery system is a new way to distribute  
5 books to bookstores, public libraries, schools and consumers. The technological  
6 breakthroughs of this invention provide a secure electronic system for both delivering  
7 selected books and receiving payments. The system has an unusual combination of  
8 features that provides the consumer with a daily use household appliance that has a high  
9 tech aura while being very practical, portable, and easy to use.

10 An advantage of the system is that it eliminates the distribution of any physical  
11 object such as a paper book or computer memory device from any book or text  
12 distribution system. The purchase of a book becomes a PAY-PER-READ event avoiding  
13 the overhead, middle-men, printing costs, and time delay associated with the current book  
14 distribution system. Published material and text such as the President's speech, a new  
15 law, a court decision on abortion, or O.J. Simpson's testimony can be made immediately  
16 available to the consumer at a nominal fee. Alternatively, books may be made available  
17 free to the end use consumer, subsidized by advertisers who sponsor books or embed  
18 advertising within the books.

19 The system is a novel combination of new technology involving the television,  
20 cable, telephone, and computer industries. It utilizes high bandwidth data transmissions,  
21 strong security measures, sophisticated digital switching, high resolution visual displays,  
22 novel controls, and user friendly interface software.

23 The primary components of the text delivery system are the subsystem for  
24 preparing the text for secure delivery and the subsystem for receiving and selecting text  
25 that was delivered. An embodiment of the system includes additional components and  
26 optional features that enhance the system. The system may be configured for use by  
27 bookstores, public libraries, schools and consumers. In one embodiment, the system for  
28 consumer use is made up of four subsystems, namely: (1) an operations center, (2) a

1 distribution system, (3) a home subsystem including reception, selection, viewing,  
2 transacting and transmission capabilities, and (4) a billing and collection system.  
3 Alternative configurations of the system are defined to allow for a variety of traditional  
4 and non-traditional delivery methods.

5 The operations center performs several primary functions: manipulating text data  
6 (including receiving, formatting and storing of text data), security encoding of text,  
7 cataloging of books, providing a messaging center capability, and performing uplink and  
8 secure delivery functions. In one embodiment, the system delivers the text from the  
9 operations center to consumer homes by inserting text data within analog video signals.  
10 The insertion of text is generally performed with an encoder at an uplink site that is  
11 within or near the operations center. The system can use several lines of the Vertical  
12 Blanking Interval (VBI), all the lines of the analog video signal, a digital video signal or  
13 unused portions of bandwidth to transmit text data. Using the VBI delivery method, the  
14 top ten or twenty book titles may be transmitted with video during normal programming  
15 utilizing existing cable or broadcast transmission capability without disruption to the  
16 subscriber's video reception. Using the entire video signal, thousands of books may be  
17 transmitted within just one hour of air time. Nearly any analog or digital video or data  
18 distribution system may be used to deliver the text data. The text data may also be  
19 transmitted over other low and high speed signal paths including a telephone network  
20 (e.g., a public switched telephone network) having a high speed connection such as an  
21 asynchronous digital subscriber line (ADSL) connection and the Internet, for example.  
22 The text data is delivered in a secure fashion over the distribution systems.

23 The home subsystem performs at least four functions: connecting to the  
24 distribution system, selecting text, storing text, and transacting through a communicating  
25 mechanism. The components of the home subsystem may be configured in a variety of  
26 hardware configurations. Each function may be performed by a separate component, the  
27 components may be integrated, or the capability of existing cable set top converter boxes,  
28 computers, and televisions may be utilized. A connector, library unit and viewer unit

1 may be used. In one embodiment, the connector portion of the home subsystem receives  
2 an analog video signal and strips or extracts the text from the video. The home library  
3 stores the text signal, provides a user friendly software interface to the system and  
4 processes the transactions at the consumer home. The viewer provides a screen for  
5 viewing text or menus and novel user friendly controls. Alternative embodiments are  
6 presented that support the secure delivery and storage of text using a variety of  
7 communication and security mechanisms.

8 The viewing device may be a portable book shaped viewer which securely stores  
9 one or more books for viewing and provides a screen for interacting with the home library  
10 unit. A high resolution LCD display is used to both read the books and to interact with  
11 the home library software. In one embodiment, an optional phone connector or  
12 return-path cable connection initiates the telephone calls and, with the aid of the library,  
13 transmits the necessary data to complete the ordering and billing portion of the consumer  
14 transaction. Alternative embodiments are presented in the referenced related applications  
15 that support ordering and billing using a variety of communication mechanisms. The  
16 user-friendly controls include a bookmark, current book and page turn button. The  
17 billing and collection system performs transaction management, authorizations,  
18 collections and publisher payments automatically.

19 A system similar to the system for consumer use may be used in bookstores,  
20 schools and public libraries.

21 The electronic books are delivered from an operations center or other remote  
22 location to an end-user location such as a home system using security mechanisms that  
23 prevent unauthorized access to the electronic books. An asymmetric public key  
24 encryption technique may be used by the operations center, serving as a sending party.  
25 The operations center encrypts the electronic book using a symmetric key and a  
26 symmetric key encryption algorithm. The symmetric key may be randomly generated,  
27 or the symmetric key may be previously defined and retrieved from storage. The  
28 operations center then encrypts the symmetric key. The encrypted electronic book and

1 the encrypted symmetric key are delivered to the home system. The home system  
2 decrypts the encrypted symmetric key and uses the symmetric key to decrypt the  
3 encrypted electronic book.

4 In another embodiment, only symmetric key encryption is used to protect the  
5 electronic book during delivery. A third party trusted source may provide a symmetric  
6 key to both the party sending the electronic book and the party receiving the electronic  
7 book. The trusted source encrypts the symmetric key using a symmetric key of the  
8 sending party and delivers the encrypted symmetric key to the sending party. The sending  
9 party decrypts the symmetric key and uses the decrypted symmetric key to encrypt the  
10 electronic book. The receiving party, which also receives the symmetric key from the  
11 trusted source in an encrypted format, decrypts the symmetric key using the receiving  
12 party's symmetric key. The receiving party then uses the decrypted symmetric key from  
13 the trusted source to decrypt the electronic book.

14 In another embodiment, the sending party and the receiving party negotiate a  
15 shared key for use in the delivery of the electronic book. The parties exchange key  
16 negotiation information and use the same key generation algorithm to generate the same  
17 key.

18 In yet another embodiment, a seed key generation algorithm is used to generate  
19 a sequence of encryption keys.

20 In an embodiment, the encrypted electronic book is broadcast to home systems.  
21 In another embodiment, the encrypted electronic book is provided on demand. In yet  
22 another embodiment, the encrypted electronic book is provided on a physical storage  
23 medium such as a smart card.

24 The system for providing secure electronic book delivery may also include  
25 integrity checking algorithms to ensure the electronic book was not altered in route. The  
26 system may also include mechanisms that identify the sending party and the receiving  
27 party.

Secure delivery of electronic books may be provided between a content provider such as a publisher and a distribution center such as an operations center. Secure delivery may also be provided between the operations center and a home system, between the home system library and the home system viewer, between a lending facility such as a public library and a home system, and between multiple viewers.

The system may also incorporate copyright protection mechanisms including application of visible copyright notices to the delivered electronic books. Other copyright information may be embedded within the electronic book using a visible watermark, for example.

#### Brief Description Of Drawings

Figure 1a is a block diagram of the primary components of an electronic book selection and delivery system.

Figure 1b is a block diagram of an electronic book selection and delivery system that uses a composite video signal.

Figure 2 is a schematic showing an overview of the electronic book selection and delivery system.

Figure 3 is a schematic of a delivery plan for the electronic book selection and delivery system.

Figure 4 is a block diagram of the operations center.

Figure 5a is a flow diagram of processing at the operations center and uplink.

Figure 5b is a block diagram of a hardware configuration for an uplink site.

Figure 6a is a block diagram of a hardware configuration for a four component home subsystem.

Figure 6b is a schematic of a two unit home subsystem.

Figure 7 is a flow diagram of processes performed by a video connector.

Figure 8 is a block diagram for an example of a library unit.

Figure 9 is a flow diagram of processes performed by a library unit on the received data stream.

1           Figure 10 is a flow diagram of processes performed by a library unit on  
2 information requests from a viewer.

3           Figure 11 is a block diagram showing the components for an example of a viewer.

4           Figure 12 is a flow diagram of processes performed by a viewer on an information  
5 request from a subscriber.

6           Figure 13 is a chart depicting a menu structure and sequencing of menus in a  
7 menu system.

8           Figure 14a is a schematic of an introductory menu.

9           Figure 14b is a schematic showing an example of a main menu.

10          Figures 14c, 14d, 14e, 14f, 14g, 14h, 14i and 14j are schematics showing  
11 examples of submenus.

12          Figure 15 is a schematic diagram of an electronic book system for a bookstore or  
13 public library.

14          Figure 16a and Figure 16b are schematics of hardware modifications or upgrades  
15 to a set top converter.

16          Figure 17 is a schematic showing a set top terminal that includes a data receiver  
17 and data transmitter.

18          Figure 18a is a schematic of a book-on-demand system.

19          Figure 18b is a schematic of an operations center supporting a book-on-demand  
20 system.

21          Figure 19a is a diagram of symmetric key encryption.

22          Figure 19b is a diagram depicting asymmetric encryption using a private key.

23          Figure 19c is a diagram depicting asymmetric encryption using a public key.

24          Figure 20 is a depiction of public key encryption for electronic book distribution.

25          Figure 21 is a depiction of symmetric key encryption for electronic book  
26 distribution where a certificate authority provides the encryption key.

27          Figure 22 is a depiction of symmetric key encryption for electronic book  
28 distribution where a certificate authority is provided the encryption key.

1 Figure 23a is a diagram depicting asymmetric encryption using a private key for  
2 an entire transaction stream.

3 Figure 23b is a diagram depicting asymmetric encryption using a public key for  
4 an entire transaction stream.

5 Figure 23c is a diagram of symmetric key encryption for an entire transaction  
6 stream.

7 Figure 24a depicts transaction key negotiation process.

8 Figure 24b depicts seed key negotiation process.

9 Figure 25a depicts a secure method for broadcast distribution.

10 Figure 25b depicts a secure method for group distribution.

11 Figure 26 depicts a hashing function process.

12 Figure 27 depicts a sender initiated, sender identification process.

13 Figure 28 depicts a recipient initiated, sender identification process.

14 Figure 29 depicts a recipient authentication sequence.

15 Figure 30 depicts a secure delivery process.

16 Figure 31 depicts a recipient initiated, secure socket layer exchange.

17 Figure 32 depicts a sender initiated, secure socket layer exchange.

18 Figure 33 depicts a reception verification sequence.

19 Figure 34 depicts driver level secure storage.

20 Figure 35 depicts file level secure storage.

21 Figure 36 depicts an operations center to home system delivery process.

## 22 Detailed Description Of Invention

23 Figure 1a shows an electronic book distribution system 100 that may be used for  
24 secure distribution of an electronic book. A content provider 110 may publish hard copy  
25 versions of books or other printed media including newspapers, magazines, and product  
26 catalogs, for example. The content provider 110 may convert printed materials to an  
27 electronic format, apply security mechanisms, and provide the electronic formatted  
28 materials to a distribution center 120, over uplink path 115. The uplink path 115 may be



1 a wired or a wireless path. The uplink path 115 may be a telecommunications network,  
2 for example. The uplink path 115 may be a satellite relay path or a wireless telephone  
3 path. The uplink path 115 may involve providing electronic books to the distribution  
4 center on a fixed media, such as a CD-ROM, for example.

5 In Figure 1a, the content provider 110 and the distribution center 120 are shown  
6 as separate components of the electronic book distribution system 100. However, the  
7 content provider 110 and the distribution center 120 may be co-located.

8 The distribution center 120 may convert printed matter into an electronic format.  
9 Alternately, the distribution center 120 may receive electronic files from an outside  
10 source, such as the content provider 110. The distribution center 120 may process and  
11 store electronic books using secure techniques as presented in Section VII.

12 The distribution center 120 distributes electronic books. The distribution may be,  
13 for example, over distribution path 125, distribution network 130, and distribution path  
14 135 to an electronic book subsystem or terminal 140, which may include an electronic  
15 book viewer (not shown). The terminal may also be a television, a set top terminal, a  
16 personal computer, or similar device. An apparatus and method for the secure  
17 distribution of electronic books is disclosed in greater detail later. The distribution  
18 network 130 may be an electronic book store, an Internet web site, a wired or wireless  
19 telecommunications network, an intranet, a radio program delivery system, a television  
20 program delivery system, including cable television, satellite television broadcast, and  
21 over-the-air broadcast, for example. The electronic book distribution network 130 could  
22 include direct delivery through a mail delivery system of electronic books on a fixed  
23 media, such as a CD-ROM, for example.

24 Figure 1b shows components of an electronic book distribution system 170 using  
25 a television program delivery system to distribute electronic books.

26 In the embodiment shown in Figure 1b, the components of the electronic book selection  
27 and delivery system 170 are an encoder 174, a video distribution system 178, a connector  
28 182, and a text selector 186. The encoder 174 places textual data on a video signal to

form a composite video signal. Although the composite signal may contain only textual data, it usually carries both video and textual data. A variety of equipment and methods may be used to encode text data onto a video signal. The video distribution system 178 distributes the composite video signal from the single point of the encoder 174 to multiple locations, which have connectors 182. The connector 182 receives the digital or analog video signal from the video distribution system 178 and separates, strips or extracts the text data from the composite video signal. If necessary, the extracted text data is converted into a digital bit stream. The text selector 186 works in connection with the connector 182 to select text.

Using the connector 182 and text selector 186 combination, various methods of selecting and retrieving desired text from a composite or video signal are possible. Text may be preselected, selected as received or selected after being received and stored. One method is for the connector 182 to strip or extract all the text from the video signal and have the text selector 186 screen all the text as received from the connector 182. The text selector 186 only stores text in long term or permanent memory if the text passes a screening process described below.

Figure 2 shows another embodiment of an electronic book selection and delivery system 200. The delivery system 200 includes: an operations center 250 including an uplink site 254, a video distribution system 208, a home system 258 including a video connector 212, a library 262, a viewer 266, and a phone connector 270, telephone system 274, an Internet web site 279 and a billing and collection system 278. Also as shown in Figure 2, the home system 258 may include connections to a television 259 and a personal computer 261 may be used to display menu screens, electronic books, electronic files, or any other information associated with the electronic book delivery system 200. In addition, the television 259 and the personal computer 261 may provide control functions that replicate and supplement those of the viewer 266.

The operations center 250 receives textual material from outside sources 282 such as publishers, newspapers, and on-line services. Alternately, the outside sources may

1 maintain electronic books at the Internet web site 279. The outside sources 282 may  
2 convert textual and graphical material to digital format and apply security mechanisms,  
3 or may contract with another vendor to provide this service. The operations center 250  
4 may receive the textual and graphical material in various digital formats and may convert  
5 the textual material to a standard compressed format for storage. In so doing, the  
6 operations center 250 may create a pool of textual material that is available to be  
7 delivered to the home system 258. The textual material may be grouped by books or  
8 titles for easy access.

9 As used herein, "book" means textual or graphical information such as contained  
10 in any novels, encyclopedias, articles, magazines, newspapers, catalogues, periodicals,  
11 or manuals. The term "title" may represent the actual title assigned by an author to a  
12 book, or any other designation indicating a particular group, portion, or category of  
13 textual information. The title may refer to a series of related textual information, a  
14 grouping of textual information, or a portion of textual data. For example, "Latest  
15 Harlequin Romance", "Four Child Reading Books (Ages 10-12)," "Encyclopedia  
16 'BRITANNICA'™," "President's Speech," "Instruction Manual," "Schedule of 4th of July  
17 Events," "Pet Handbooks," "Roe v. Wade," and "The Joy of Cooking," are suitable titles.  
18 Also, the title may be a graphical symbol or icon. Thus, a picture of a wrench may be a  
19 title for a repair book, a picture of a computer a title for a computer book, a graphical  
20 symbol of a telephone a title for a telephone book, a drawing of a dagger a title for a  
21 mystery book, a picture of a bat and ball a title for a sports book, and a picture of  
22 tickertape a title for a business book.

23 The operations center 250 includes the uplink site 254 for placing the text onto  
24 a telecommunications signal in a secure fashion and sending the telecommunications  
25 signal into a distribution system. The uplink site 254 would generally include an encoder  
26 204 (not shown in Figure 2) to encode the text onto the telecommunications signal.

27 Many analog and digital video distribution systems may be used with the  
28 electronic book delivery system 200, such as cable television distribution systems,

1 broadcast television distribution systems, video distributed over telephone systems, direct  
2 satellite broadcast distribution systems, and other wire and wireless video distribution  
3 systems. Nearly any distribution system which can deliver a telecommunications signal,  
4 including a video signal, will work with the electronic book delivery system 200. It is  
5 also possible to distribute the electronic book without using a telecommunications signal  
6 as described in the embodiments presented in the referenced related applications.  
7 Methods used for securing the distribution of materials over the electronic book delivery  
8 system 200 are presented in Section VII.

9 The home system 258 performs five functions: (1) connecting with a video  
10 distribution system; (2) selecting data; (3) storing data; (4) displaying data; and (5)  
11 handling transactions. An important optional function of the home system 258 is  
12 communicating using, in one embodiment, a telephone communication system 274. The  
13 home system 258 may be made up of four parts: a video connector 212 or similar type  
14 of connector for connecting with the distribution system 208, a library 262 for storing and  
15 processing, a viewer 266 for viewing menus and text and a telephone connector 270 for  
16 connecting with a telephone communications system 274. Additional embodiments are  
17 presented in the referenced related applications that address alternative communication  
18 mechanisms.

19 The billing and collection system 278 may be co-located with the operations  
20 center 250 or located remote from the operations center 250. The billing and collection  
21 system 278 may be in communication with the home system 258 using telephone-type  
22 communication systems (for example 274). Any of a number of communication systems  
23 as presented in the referenced related applications, such as a cellular system or the  
24 Internet, will operate with the billing and collection system 278. The billing and  
25 collection system 278 records the electronic books or portions of text that are selected or  
26 ordered by the subscriber. The collection system will charge a subscriber's credit account  
27 or bill the subscriber. In addition, the billing and collection system 278 may monitor that

1 amount due to publishers or other outside sources 282 who have provided textual data  
2 or other services such as air time to enable the text delivery system 200 to operate.

3 Also shown in Figure 2 is an intranet 279'. The intranet 279' may be used as a  
4 part of a private distribution network for distributing and circulating electronic books.  
5 For example, a university library may use the intranet 279' to circulate electronic books  
6 to university students and professors.

7 Figure 3 is an expanded overview of a delivery plan 301 for the electronic book  
8 delivery system 200. It is a comprehensive delivery plan 301 to support various types of  
9 users and various billing systems. Figure 3 shows that publishers 282 may provide text  
10 transfer 302 to the operations center 250' and receive payments 306 from the billing and  
11 collection system 278'. A separate channel uplink site 254' is shown in this configuration  
12 receiving data 310 from the operations center 250'. The operations center 250' has three  
13 separate sections (318, 322, 326) one for text receiving, formatting and re-entry 318, a  
14 second for security encoding and processing 322 and a third section for catalog and  
15 messaging center functions 326.

16 The collection and billing system 278' shown has two sections (330, 334) one for  
17 transaction management, authorizations and publisher payments 330, and the other for  
18 customer service 334. The customer service section 334 provides for data entry and  
19 access to customer account information. Transaction accounting information 338 is  
20 supplied to credit card companies 342 by the transaction management section 330 of the  
21 billing and collection system 278'. The credit card companies 342 provide billing 346 to  
22 customers either electronically or by mail.

23 Methods for communicating between the subscriber base 348 and the billing and  
24 collection system 278' include: by telephone switching 350 alone, cellular switching 354  
25 and telephone switching 350 combined, and by use of the cable system 358 and the  
26 telephone switching 350. The system shown supports both one-way 362 and two-way  
27 cable communication 366 with subscribers. Additional communication methods are  
28 presented in the referenced related applications. Public libraries and schools 370 as well

as bookstores 374 may use the delivery system 301. Methods used for securing these communications are presented in Section VII.

Public libraries and schools 370 could have a modified system to allow the viewer to be checked-out or borrowed while bookstores 374 would rent or sell the viewer and sell electronic book data. The bookstores 374 as well as the public libraries and schools 370 may be serviced by cable 378. Optional direct broadcast systems (DBS) 382 can also be used with the system 200 as detailed in the referenced related applications.

#### I. The Operations Center

Figure 4 is a schematic of the operations center 250, which includes the uplink 254. The operations center 250 may gather text or books by receiving, decrypting, formatting, storing, and encoding. A data stream 302 containing text may be received at the operations center 250 by a data receiver 402. The data receiver 402 is under the control of a processor 404. After reception, the data stream is decrypted using digital logic for decrypting 403 which is under the control of the processor 404. The data stream is then formatted using digital logic for formatting 406 which is also under the control of the processor 404. If any additional text is generated at the operations center 250 locally for insertion into the distributed signal, the text generation is handled through text generator hardware 410, which may include a data receiver and a keyboard (not shown). Following processing by the text generator 410, the additional text can be added to the text received by the combining hardware 414 that includes digital logic circuitry (not shown).

The processing at the operations center 250 is controlled by a processor 404, which uses an instruction memory 416. The processor 404 and instruction memory 416 may be supplied by a personal computer or mini-computer, for example. To perform the catalog and messaging functions, the operations center 250 uses a catalog and message memory 420 and the text generator 410 if necessary.

The data stream of text, catalog and messages may be encoded by security module encoding 424 prior to being sent to the uplink module 254. Various encoding techniques

1 may be used by the security encoding module 424 such as the commercial derivative of  
2 NSA's encryption algorithm (Data Encryption System (DES)) and General Instrument's  
3 DigiCipher II. Additional embodiments are presented in Section VII. Following  
4 encoding, the encoded text may be stored in text memory 428 prior to being sent to the  
5 uplink 254. A first-in-first-out text memory arrangement may be used under the control  
6 of the processor 404. Various types of memory may be used for the text memory 428  
7 including RAM. The operations center 250 may use file server technology for the text  
8 memory 428 to catalog and spool books for transmission as is described below. The  
9 operations center 250 may also store the electronic book as secure compressed data files  
10 using the secure storage techniques presented in Section VII.

11 In an embodiment, to transmit textual data, the distribution system 208 (see  
12 Figure 2) may use high bandwidth transmission techniques such as those defined by the  
13 North American Broadcast Teletext Standard (NABTS) and the World System Teletext  
14 (WST) standard. Using the WST format (where each line of the Vertical Blanking  
15 Interval contains 266 data bits), a four hundred page book, for example, may be  
16 transmitted during regular television programming using four lines of the Vertical  
17 Blanking Interval at a rate of approximately one book every 1.6 minutes (63,840 bits per  
18 second). Alternatively, books may be transmitted over a dedicated channel, which  
19 interrupts programming so that 246 lines of video can be used to transmit approximately  
20 2,250 books every hour (3.9 Mbits per second). A teletext type format is the simplest but  
21 possibly the slowest text format to use with the electronic book delivery system 200. In  
22 either event, an encoder 204 may be used at an uplink site 254 to insert textual data into  
23 the analog video signal. In many other respects, the delivery of the textual information  
24 may be completed using an existing cable television plant and equipment. Alternative  
25 transmit formats and delivery systems are presented in the referenced related applications.

26 Figure 5a is a flowchart of steps involved in processing text from the publisher  
27 or provider 282 that may occur at the operations center 250. As shown in block 500, the  
28 publisher 282 processes data files of text for books, compresses, encrypts and sends the

1 data files to the operations center 250 or uplink 254. Text files for books may be sent one  
2 book at a time. As shown in block 504, the uplink 254 or operations center 250 receives  
3 and processes the data stream from the publisher 282. Generally, part of this processing  
4 includes encryption and error correction. Specific embodiments used for encryption are  
5 presented in Section VII. Text files may be delivered for receipt by multiple home  
6 subsystems simultaneously, or to a specific individual home subsystem.

7 In Figure 5a, the electronic books are distributed to consumers using a video  
8 distribution system such as a cable television system. However, the electronic books may  
9 also be packaged as data packets and distributed over other telecommunications networks  
10 such as a digital wireless telephone network, for example.

11 In one embodiment, as shown in block 508, files are broken into smaller packets  
12 of information. Header information is added to the packets. The bit stream is converted  
13 from a serial digital bit stream to an analog bit stream that is compatible with an NTSC  
14 video signal. Block 512 shows the switching of analog data into the video lines of a  
15 video signal. The analog data may be placed either in the VBI or the active video lines.  
16 In some instances, unused portions of bandwidth (such as 5-40 MHZ, 70-75 MHZ,  
17 100-109 MHZ or other guard bands) may be used instead of the video lines. Alternate  
18 transmission methods are presented in the referenced related applications.

19 Figure 5b is an example of a hardware configuration to perform some of the  
20 functions for blocks 508 and 512. A video feed 516 is received and processed through  
21 a sync stripper 520. The stripped sync signal 532 is used by the digital logic control 524.  
22 The digital logic control 524 receives the sync signal 532 and a serial digital bit stream  
23 528 for processing. The digital logic control 524 passes the serial digital bit stream to the  
24 Digital to Analog converter 536 and outputs a control signal 540 for the video switch  
25 544. The video switch 544 integrates the video feed 516 and analog data stream 548 into  
26 a video feed with analog data signal inserted 552.

27 As an alternative to cable, broadcast or other television delivery methods, the  
28 public telephone system may be used to transmit books to the subscribers. An average



1 book would take about 7 minutes to transmit over the public telephone system. Using the  
2 telephone system, it is not necessary to combine video and text into a composite signal.  
3 In most other respects, the operations center would remain similar whether text delivery  
4 was by telephone or cable. File server technology (such as that described in U.S. Patent  
5 No. 5,262,875, entitled AUDIO/VIDEO FILE SERVER INCLUDING DECOM-  
6 PRESSION/ PLAYBACK MEANS, issued to Mincer, et al., and, U.S. Patent No.  
7 5,218,695, entitled FILE SERVER SYSTEM HAVING HIGH-SPEED WRITE  
8 EXECUTION, issued to Noveck, et al., incorporated herein by reference) may be used  
9 at the operations center with a telephone system text delivery method.

10 As another alternative to cable, television, and telephone system delivery, the  
11 public telephone system may be used to provide access to the Internet, where the Internet  
12 web site 279 may be accessed. Electronic books may be ordered, paid for, and delivered  
13 directly from the Internet web site 279 over the telephone system. In addition, the  
14 electronic book viewer 266 may be used for wireless voice and data communications  
15 using the Internet.

16 When a wireless telephone network is used to distribute electronic books, or  
17 otherwise communicate with the home system 258, the home system 258 may receive  
18 data using any one or more standard protocols including time division multiple access  
19 (TDMA), code division multiple access (CDMA), Global Systems for Mobile  
20 Communications (GSM) and Advanced Mobile Telephone System (AMPS) protocols.  
21 In any delivery system using the telephone system, individual subscribers may increase  
22 the electronic book deliver rate by incorporating high speed modems or other  
23 communications devices such as an Integrated Services Digital Network (ISDN)  
24 connector, or by use of a Digital Subscriber Line (DSL). These alternative delivery  
25 methods are presented in the referenced related applications.

## 26 II. The Home System

27 The hardware configuration for a four component home system 258 is shown in  
28 Figure 6a. Figure 6b shows a hardware configuration for a two component home

1 subsystem. The home system 258 performs several functions, such as receiving data and  
2 video transmissions, stripping (or extracting) the data from the video signal, decrypting  
3 the data, screening and storing the data, providing user friendly interface controls and  
4 software, displaying menus and text, processing transactions, initiating telephone calls  
5 and transmitting billing data. Various hardware configurations may be utilized to achieve  
6 the desired functions of the home system 258. For example, as shown in figure 6b, the  
7 home system 258 can be configured to utilize the reception and channel tuning capability  
8 of the current installed subscriber base of cable converter boxes and televisions 601 and  
9 networked computers. The home system 258 can also be designed as an advanced set top  
10 terminal converter box with menu generation capability, electronic memory and a  
11 telephone modem as described in section V below. Alternatively, the home system 258  
12 can be configured to support alternate delivery and ordering methods as described in the  
13 referenced related applications.

14 The electronic components which make up the home system 258 can be arranged  
15 in a variety of ways. In the four unit subsystem of figure 6a the viewer 266 and library  
16 262 are wired together while the remaining components communicate through RF  
17 transceivers 604. In a simple version of the home system 258 there are only two units,  
18 a library 262 and a viewer 266. Figure 6b shows a two unit home system 258 with certain  
19 optional features.

20 The viewer 266 is generally equipped with a high resolution viewing area 602,  
21 digital logic (including a key 605, security 606, and a microprocessor 621), video  
22 graphics control and memory 607, power supply circuitry 602 (not shown), an optional  
23 battery 603 and an optional RF transceiver 604. In a two unit arrangement, the library  
24 262 contains the connector function to the electronic book distribution system 208,  
25 connector function to a public telephone communications system, and memory 600  
26 (which may be removable and portable 600'). More specifically, the library 262 would  
27 include data stripping functions 617, digital logic 609, memory storage 600, power  
28 circuitry 610, optional connections 611 (including cellular or PCN 611'), optional battery

1 (not shown), optional tuner module 613 and an optional RF transceiver 604. The  
2 connector 212 and the public telephone system connection 270, as well as the removable  
3 portable memory unit 600 of the library 262 may be broken out into separate components.  
4 (Figure 6b shows a removable portable hard disk memory 600' with removable cartridges  
5 614.) Finally, the home system 258 may include an attached keyboard 267 or a wireless  
6 keyboard 268. Both the attached keyboard 267 and the wireless keyboard 268 may be  
7 used to communicate with the viewer 266 (not shown) or the library unit 262. The  
8 wireless keyboard 268 may communicate using radio frequency (RF) signaling, for  
9 example.

10 In an alternate arrangement, all functions of the home system 258 may be  
11 incorporated into a single unit. The functions of the library 262, for example, may be  
12 carried out by a card or chipset in the viewer 266. All the communications devices  
13 needed to couple the home system 258 to various telecommunications networks may also  
14 be incorporated into the viewer. All interfaces between the home system 258 and the  
15 subscriber may be included with the viewer 266. In this embodiment, the viewer 266  
16 may include a communication device for receiving inputs from a separate keyboard. The  
17 viewer 266 may also include a built-in video camera 608" that may be used to transmit  
18 images of the subscriber. Using the transceiver 608, the camera 608" and the  
19 speaker/microphone 608', the subscriber may use the viewer 266 for video conferencing,  
20 for example.

21 Therefore, the home system 258 may have as many as five separate components,  
22 which communicate with each other. The two, three, four or five separate components  
23 which make up the home subsystem can communicate with each other in a variety of  
24 ways, including hardwired connection 615, RF transceiver 604 and other wireless  
25 methods.

26 RF communications may be used in the home, allowing separate components to  
27 be located throughout the home without restriction. The data communicated between the  
28 units may be secure data using security techniques presented in Section VII. In addition,

1 the library 262 may provide power to the viewer 266 through the hard wire  
2 communication link 615.

3 To receive and strip data from a video signal at the consumer's home, a device  
4 such as a cable interface device or cable connector 212 is used. The cable connector  
5 device includes a tuner 613, while the cable interface device makes use of existing tuning  
6 equipment in the home. In either configuration, data is stripped from the video signal  
7 and stored at the subscribers location in the library 262. The phone connector 270,  
8 optional connector 611, and modular connector 701 initiate communications and transmit  
9 ordering and billing information to the operations center 250 or billing and collection  
10 system 278. A digital connector 619 is provided to communicate digital information with  
11 the set top 601. The library 262 is the intelligent component of the home subsystem,  
12 incorporating the hardware and software necessary to store the text data, generate menus  
13 and effect the purchase transactions. In addition to an RF transceiver 604, the home  
14 library 262 also includes the necessary jacks and connections to allow the system to be  
15 connected to the viewer 266. As shown in Figure 6b, the library 262 communicates the  
16 text data to the viewer 266 in a secure format, which requires a key 605 for decryption.  
17 The text may be decrypted page by page just before viewing. Alternative security  
18 embodiments for library 262 to viewer 266 communications are presented in Section VII.

19 a. The Video Connector

20 Figure 7 shows the flow of the processes performed by the video connector 212.  
21 The video connector 212 receives the video signal 608, tunes to the channel containing  
22 the text data 612, strips the text data from the video signal 616, and communicates the  
23 text data stream to logic components in the library 622.

24 The connection to the video distribution system may be a cable connector to a  
25 cable television delivery system, as shown in Figure 6b. The cable connector includes  
26 a data stripper circuit 617, which accepts video input from either a set top converter, TV  
27 or VCR 601, or an optional tuner block 613 that receives the CATV signal through the  
28 cable connector 212'. The data stripper circuit 617 strips data out of the video, and

1 outputs a digital bit stream to the digital logic portion 609 of the library unit 262. The  
2 data is embedded in the video signal either in the vertical blanking interval or the active  
3 video portion in an encrypted and compressed format. The data stripper circuit 617 can  
4 be placed inside the set top converter box 601, TV, or in the library 262. The data  
5 stripper circuit 617 outputs the digital bit stream to be used by the library digital logic  
6 609.

7 The video connector 212 may also contain a channel tuner module 613 that can  
8 tune to the video channel and provide access to the video that contains the data to be  
9 stripped. Using the optional tuner module 613, a set top converter, VCR, or TV tuner is  
10 not needed in the home system 258. The optional tuner module 613 would instead  
11 receive the CATV signal directly through the cable connector 212. Additional connector  
12 options, which allow for the receipt of text files using alternative delivery methods, are  
13 presented in the referenced related applications. This ubiquitous access is provided using  
14 the modular connector 700 as depicted in Figure 6b.

15 b. Library

16 An embodiment of the library 262 for a two unit home subsystem is shown in  
17 both Figure 6b and Figure 8. The embodiment shown includes the following optional  
18 parts: the video connector 212, phone connector 270, RF transceiver 604, and battery  
19 pack 624 in addition to a removal portable memory 600', microprocessor 628, instruction  
20 memory unit 632, digital logic 636, and power unit 640.

21 The library 262 contains a digital logic section 609 (not shown in Figure 8) which  
22 includes the microprocessor 628, the digital logic 636 and the instruction memory unit  
23 632. The microprocessor 628 may be a secure microprocessor such as the Mot SC21  
24 device sold by Motorola. The digital logic section 609 will receive the serial digital bit  
25 stream from the data stripper circuit 617 and process the data. Error correction and  
26 security processing will also be performed by the digital logic section 609 and the data  
27 will be checked for proper address. If the address of the data is correct and the library  
28 262 is authorized to receive the data, the data will be decrypted and transferred to the

1 memory storage unit 600, 600'. Authorization to receive the data may be provided by the  
2 cable headend or another distribution point. An authorization code may be sent in the  
3 serial digital bit stream. The digital logic section 609 will send appropriate text and  
4 graphical data to the memory storage unit 600, 600'. It may decrypt then re-encrypt the  
5 data or transfer this data in a compressed and encrypted format and the data remains  
6 stored in a compressed and encrypted format.

7 i. Memory Storage Unit

8 The memory storage unit of the library may be a removable portable memory unit  
9 600' (as shown in Figures 6a, 6b and 8). A variety of options are available for memory  
10 storage: a hard disk drive, such as an 80 megabyte, a 200 megabyte, a hard disk with  
11 removable platters, and CD ROM. Referring to Figure 6b, a hard disk drive unit 600',  
12 which contains removable platters, may also be used. This would provide virtually  
13 unlimited library storage capacity. Data may be stored in the memory storage unit in a  
14 compressed and encrypted format. As is also shown in Figure 6b, the data may also  
15 contain a key or unique ID number that matches the ID or key of the viewer 266. This  
16 matching of a unique key or ID number prevents unauthorized transfer of text data from  
17 the memory storage unit to an unauthorized viewer. Alternative embodiments to store  
18 text data in encrypted format are addressed in Section VII. Small memory devices such  
19 as smart cards, electronic memory cards or PCMCIA cards (personal computer memory  
20 card industry association) may also be used to store the data.

21 ii. Power Circuitry

22 As shown in figures 6b and 8, the library 262 will accept power from AC wall  
23 power 610, DC power 640, or optional battery power 624. The power circuitry 610, 640  
24 may provide all the voltage necessary from either the battery 624 or AC unit for the  
25 various circuitry in the library. The power circuitry 610, 640 may also provide power to  
26 the viewer through a single data cable when connected to the viewer. The power circuitry  
27 610, 640 will recharge the battery using AC power when in operation. With the optional  
28 battery unit 624 installed, the library 262 becomes a portable unit and can still provide

1 power to the viewer 266. In order to extend battery life, power conservation measures  
2 may be utilized, such as shutting down the memory system when not in use. When the  
3 viewer unit 266 is being utilized and the library circuitry is not being utilized, virtually  
4 all power may be shut down to the library 262.

5 iii. Connection to the Public Telephone System

6 In an embodiment, the connection to the telephone system may be provided by  
7 a connector device 611, which consists of a modem. Various available modems may be  
8 used to perform this function. As shown in Figure 6b, cellular phone or PCN phone  
9 connections 611' may also be provided. When the home system 258 is first initialized,  
10 the modem may be used to transfer the name and credit card information of the consumer  
11 to the billing and collection system 278. The telephone connection 270 may be utilized  
12 each time an electronic book is purchased by a consumer to complete and record the  
13 transaction. The telephone connection 270 may also be used to receive the text data from  
14 the operations center 250, by-passing the video distribution system 208. The phone  
15 connection 270 may be a separate unit as shown in Figure 6b. However, alternate means  
16 exist to connect the home system 258 to the billing and collection system 278 or the  
17 operations center 250. The modular connector 701 (shown in Figures 6b and 8) provides  
18 access to each communication network to provide a path from the home system 258 to  
19 the billing and collection system 278 or the operations center 250. These alternatives are  
20 presented in detail in the referenced related applications.

21 iv. Library Processing

22 Figure 9 shows for one embodiment, an example of processing performed by the  
23 digital logic section 609 of the library 262 on the data stream 651 received from the video  
24 connector 212 or stripper circuit 617. In step S650, digital logic section 609 checks the  
25 data stream 651 for error correction. If an error is detected, in step S654 digital logic  
26 section 609 de-interleaves the data and in step S658 runs a FEC (Forward Error  
27 Correcting) algorithm. In steps S650, S654 and S658, the digital logic section 609  
28 performs the error correction needed on the data stream. If no error correction is

1 necessary the digital logic section 609 proceeds to step S662 and checks data packets  
2 individually for packet address.

3 If the address is a unique address, the process moves to step S666 and the digital  
4 logic section 609 checks whether the address of the packet matches the library box ID  
5 number. The library box ID number is a unique number associated with the library 262.  
6 The library box ID is used to ensure security of the data. The process then moves to Step  
7 S668, and the digital logic section 609 performs the decryption processing, as presented  
8 in Section VII. The process then moves to step S670 and the digital logic section 609  
9 determines whether an electronic file has already been opened into which the data packet  
10 can be saved. If no data file has been opened, the digital logic section 609 opens a new  
11 data file for that packet. If an electronic file has been opened, the process moves to step  
12 S678 and the digital logic section 609 saves the packet in the electronic file on disk. The  
13 process moves to step 682 and the digital logic section 609 checks to see if this is the last  
14 packet for a particular book for a particular textual data block being received. If it is the  
15 last packet of information, the process moves to step 686 and the digital logic section 609  
16 closes the electronic file and updates the directory of available electronic files. Following  
17 either step S682 or S686, the process returns to receive another data packet from the data  
18 stream received from the data stripper block.

19 If the packet address is checked and the address is determined to be a broadcast  
20 address, the process moves to step S690 and the digital logic section 609 determines the  
21 type of message that is being sent. The message may be an index of book titles, menu  
22 (and menu graphics) information, announcements, special offerings, discounts,  
23 promotions, and previews, for example. The process then moves to step S694 and the  
24 digital logic section 609 stores the message in an appropriate electronic message file.  
25 The process then returns to step S650 to receive another data packet and perform another  
26 error check.

27 Using the process of Figure 9, the library 262 is able to receive, store and update  
28 directories related to the textual data and graphical data (that can be used to depict



1 pictures in a given book or to generate menus). Variations of the processes are possible  
2 depending on the format of the data and operating system of the library 262.

3 Figure 10 shows an example of the processing of information requests from the viewer  
4 266 at the library 262. Information requests from the viewer 266 are received either  
5 through the cable connecting the viewer 266 to the library 262 or through wireless  
6 transmissions such as RF. It is possible in some embodiments for subscribers' requests  
7 to come from a set top converter box 602 (see Section V).

8 Information requests received from the viewer 266 generally fall into three  
9 categories: (1) directory data of books stored in the library 262, (2) index of all available  
10 books on the system, and (3) requests for a specific book (step S700). In step S704, the  
11 digital logic section 609 answers a request from the viewer 266 for a directory of data  
12 showing the books stored at the viewer 266. The directory of data is sent to the viewer  
13 266 so that it may be displayed to the subscriber. In step S708, the digital logic section  
14 609 handles requests from the viewer 266 for an index of all available books on the  
15 system. The library 262 will obtain an index of all the available books on the system and  
16 transmit that index, in step S712, with menu information to the viewer 266. In step S716,  
17 the digital logic section 609 replies to a request from the viewer 266 for a specific book.  
18 In step S720, the digital logic section 609 opens an electronic file for the specific book  
19 requested by the viewer 266 and transmits the record or transmits the information on a  
20 packet-by-packet basis to the viewer 266. This process of transmitting the specific book,  
21 record, or packets to the viewer 266 continues until the last record or packet has been sent  
22 in step S724.

23 In addition to the processes shown on Figure 10 in handling a request for a  
24 specific book, the library 262 also orders and receives specific books from the operations  
25 center 250 using the process as described in step S716. Following a request for a specific  
26 book which is not stored at the library 262, the library 262 will proceed to determine the  
27 next available time the book will be on the video distribution system 208 or an alternative  
28 delivery system and ensure reception and storage of that book (process not shown). In

1 performing this process the library 262 will transmit to the viewer information on when  
2 it will obtain the text data for the book so that the subscriber may view the book. In  
3 addition to timing information, price and other ordering information may also be passed  
4 by the library 262 to the subscriber.

5 c. The Viewer

6 Figure 11 is a block diagram of a viewer 266 showing its internal components.  
7 The viewer 266 of Figure 11 is similar to the viewer 266 depicted in Figure 6b. The  
8 viewer 266 is designed to physically resemble a bound book. The viewer 266 is made  
9 up of five primary components and seven optional components: (1) LCD display 602,  
10 (2) digital circuitry (not shown), (3) video graphics controller 607N, (4) controls 740, (5)  
11 book memory 728, (6) optional power supply circuitry 736, (7) optional battery 603N, (8)  
12 optional RF transceiver 604, and (9) optional cellular or mobile connector (such as 611N)  
13 (10) optional keyboards 267 and 268, and (11) an optional speaker/microphone 608', (12)  
14 optional alternative communication interface devices.

15 (1) A high resolution LCD screen 602, of VGA quality, may be used by the  
16 viewer 266 to display text and graphic images. The screen may be the size of one page  
17 of an electronic book. A two page screen or two screens may also be used with the  
18 viewer 266.

19 (2) Digital circuitry that includes a secure microprocessor 621, instruction  
20 memory 732, and digital logic. Data is transferred to the viewer 266 in compressed and  
21 encrypted format. In one embodiment, the secure microprocessor 621 compares the ID  
22 number of the viewer 266 with the incoming data stream and only stores the text data if  
23 the ID number of the viewer 266 matches that within the incoming data stream. The  
24 viewer 266 may be configured to not output text data or other data and that the data is  
25 decompressed and decrypted only at the moment of viewing and only for the current page  
26 being viewed. These measures provide additional security against unauthorized access  
27 to data. Additional embodiments are presented in Section VII.

(3) A video graphics controller 607' that is capable of assisting and displaying VGA quality text and graphic images is included in the viewer 266. The graphics controller 607' is controlled by the digital circuitry described above. Text may be displayed in multiple font sizes.

(4) The viewer 266 of Figure 11 has touch panel controls 740. These unique and novel controls 740 allow the consumer to select stored electronic books and electronic books from catalogues, move a cursor, and turn pages in an electronic book. Typically, the controls 740 include forward and reverse page buttons 742, 741, a ball 743 for cursor movement, one or more selection buttons 745, a current book button 747 and a bookmark button 749 (see Figure 14a).

The controls 740 should be easy to use and conveniently located. Referring to Figure 14a, the controls for the viewer 266 may be located below the screen 602 at the bottom portion of the viewer 266. The next page turn button 742 is the most used button 740 and is located towards the right edge of the page. The subscriber is likely to use right hand thumb movements to work the controls particularly the page turn buttons 741, 742. Therefore, the buttons may be arranged in such a manner that the buttons are easily controlled by a subscriber's right thumb. Generally, this can be accommodated either on the lower portion of the viewer 266 (as shown) or along the right hand margin of the viewer 266 (not shown). The current book button 747 and bookmark button 749 are usually the least used of the controls 740. Therefore, in the example shown, those buttons 747, 749 are located on the inside portion towards the binder of the viewer 266.

Locating the ball 743 or other cursor movement device (such as four pointer arrows not shown) in the bottom center of the viewer 266 is both easier for the subscriber to use and easier in manufacturing the viewer 266. The selection buttons for the cursor 745 may be located below the middle diameter of the cursor ball 743 on the right and left sides of the ball as shown. If pointer arrows are used for cursor movement, a selection button 745 may be located in the center of the four arrow buttons (not shown). Again,

1 the most used controls 740 should be located where a subscriber's right hand thumb  
2 would normally rest.

3 (5) Book memory 728 for at least one electronic book or more of text is  
4 included in the viewer 266. The memory 728 stores text and any graphics, which  
5 represent pictures in a book. The memory 728 can also store menu graphics data. Two  
6 different memory 728 devices may be used in the viewer 266, one for the instructions for  
7 the microprocessor 621 in the digital circuitry and a second type of memory may be used  
8 for the book memory 728 (and graphics). Various memory devices available on the  
9 market may be used such as, ROM, RAM or a small hard disk. Since an electronic book  
10 requires approximately 0.6 megabytes of storage, a small hard disk providing  
11 approximately 60 MBytes of storage provides memory to store approximately 100  
12 electronic books.

13 Text for electronic books may be displayed in various font sizes. To  
14 accommodate various fonts for display, a variety of fonts are stored in instruction 732 or  
15 book memory 728. Thus larger or smaller fonts may be recalled from memory 621, 728  
16 to create displays desired by the subscriber.

17 (6) Power supply circuitry 736 in the viewer 266 will accept power from  
18 either an AC power source or from an optional battery 603', or the library 262. The  
19 power supply circuitry 736 provides the necessary voltages to accommodate the various  
20 systems within the viewer 266.

21 (7) An optional battery 603' is provided in one embodiment. The battery 603'  
22 is automatically recharged when AC power is available.

23 (8) An optional RF transceiver 604 which provided two-way data link  
24 between the viewer 266 and other components of the home subsystem can also be  
25 included in the viewer 266.

26 (9) Also, the viewer 266 may include a cellular transceiver (not shown) for  
27 mobile communications.

(10) The optional wired (attached) keyboard 267 and wireless (e.g., RF) keyboard 268 (see Figure 6a) may be used with the viewer 266 to provide communications between the subscriber and the viewer 266.

(11) The optional speaker and microphone 608' allow the viewer 266 to provide audio signals to the subscriber, and allow the subscriber to provide an audio input. The speaker and microphone 608' may be used in conjunction with the cellular transceiver 608 or other telecommunications equipment to provide for reception and transmission of telephony and data.

(12) The optional alternative communication interface devices allow the viewer 266 to make use of a variety of communication paths, including wireless Internet paths.

The viewer 266 of Figure 11 has parts available for providing connections to: a library 744, electronic card memory 748, CD ROM units 752, and a portable memory unit 756 (such as that shown in Figure 6b as 600'). Various electronic memory cards such as PCMCIA can be used with the viewer 266 to supply and store electronic books.

Security, low power consumption and excellent display technology are desired features of the viewer 266 design. The viewer 266 should be lightweight and portable. The viewer 266 contains a software operating system that allows electronic books to be stored, read and erased and includes the capability to order electronic books and retain them in memory 728 for a predefined period of time determined by the system operator. The software can be configured to allow the electronic book to be read during a period of time (i.e., two weeks) and then automatically erased, read once and erased, or held in memory permanently. In one embodiment, each viewer 266 may have a unique key 605. All of the data storage may be encrypted with the key 605 for an individual viewer 266 to prevent more than one viewer 266 accessing the text file or electronic book file. Alternative security embodiments are presented in Section VII.

Figure 12 is a flow diagram of some of the processes executed by the microprocessor 621 in the viewer 266. The viewer 266 may receive inputs from the

1 subscriber through touch panel controls 740. In step S800, the subscriber's information  
2 requests are then processed by the microprocessor 621.

3 In step S804, if the subscriber requests a menu of available electronic books, the  
4 microprocessor 621 will select an electronic book menu. In step S808, the  
5 microprocessor 621 will open the electronic files that list the electronic books which are  
6 available (related to the category of topic of the menu) and display the menu with the  
7 names of the available electronic books.

8 If the subscriber selects a particular book to read, then in step S812, the  
9 microprocessor 621 will process the selection and determine the electronic file that  
10 contains the specific electronic book. In step S816, the microprocessor 621 will open the  
11 file for that specific electronic book and normally access the first page. (If a pointer has  
12 already been set in that books electronic file, the process may default to that page.) In  
13 step S820, the microprocessor 621 will then determine which page needs to be displayed.  
14 That is, the microprocessor 621 will determine whether a next page, previous page or a  
15 bookmarked page needs to be displayed. If the pointer for the electronic file is not in the  
16 correct location then in step S828, the microprocessor 621 will move the pointer and  
17 obtain the previous page of data from the stored file. Otherwise, in step S824, the  
18 microprocessor 621 will normally obtain the next page of text from the stored electronic  
19 file. In step S832, the microprocessor 621 decrypts the text data using one of the  
20 embodiments presented in Section VII, decompresses the text data and sends the data to  
21 the video display. The video display will generally have a video display memory  
22 associated with it. In step S832, the microprocessor 621 will send the data directly to that  
23 video display memory. The circuitry for the display then completes the process of  
24 displaying the page of text.

25 If the subscriber, through the controls 740, requests (from step S800) that the  
26 power be turned off, then in step S836, the microprocessor 621 initiates power off. In  
27 step S840, the microprocessor 621 saves the pointer in memory to the page number in the  
28 book that the viewer 266 is currently reading. In step S844, the microprocessor 621

1 closes all the electronic files and signals the power circuitry to shut down the power to  
2 the various circuits in the viewer 266. With these examples of basic processes the viewer  
3 266 is able to display book selections and display text from those electronic books.

4 d. Menu System

5 Referring generally to Figure 13, the electronic book system 200 may have a  
6 menu system 851 for selecting features and books from the electronic book system 200.  
7 The operating software and memory required for the menu system 851 may be located  
8 at the viewer 266 (e.g., the instruction memory 732 and/or book memory 728). However,  
9 it can also be located at the library 262 (e.g., the instruction memory 632) or the library  
10 262 and the viewer 266 can share the software and memory needed to operate the menu  
11 system 851. Since the menus are usually displayed on the viewer, and since the viewer  
12 266 may be capable of operating in the absence of the library 262, the basic software and  
13 memory to create the menus is more conveniently located at the viewer 266.

14 The menu system 851 allows sequencing between menus and provides menu  
15 graphics for graphical displays such as on the LCD display 602 of the viewer 266. In an  
16 electronic book system that uses a set top converter these menus may also be displayed  
17 on a television screen. In an electronic book system that uses a computer, these menus  
18 may also be displayed on the computer monitor. In an embodiment, the menus provide  
19 just basic text information from which the subscriber makes choices. In other  
20 embodiments, the menus provide visual displays with graphics and icons to assist the  
21 subscriber and allow for subscriber interaction and real-time ordering of electronic books  
22 or other content available to the subscriber.

23 Figure 13 depicts the menu system 851 with sequencing. The primary menus in  
24 the menu system 851 are an introductory menu 850, a main menu 854 and various  
25 submenus 858. In the embodiment shown, there are three levels of submenus 858. In  
26 certain instances one or two submenus 858 is sufficient to easily direct the subscriber to  
27 the selection or information requested. However, there are features in which three or  
28 more submenus 858 make the user interface more friendly for the subscriber. Each level

1 of submenus 858 may consist of multiple possible menus for display. The particular  
2 menu displayed depends on the selection by the subscriber on the previous shown menu.  
3 An example of this tree sequence of one to many menus are the help submenus 887, 888.  
4 Depending upon the specific help requested, a different level two help menu is displayed  
5 to the subscriber.

6 An example of an introductory menu 850 is shown on Figure 14a. Generally the  
7 introductory menu 850 introduces the viewer 266 to the system and provides initial  
8 guidance, announcements and instruction. The introductory menu 850 is followed by a  
9 main menu 854, an example of which is shown in Figure 14b. The main menu provides  
10 the viewer 266 with the basic selection or features available in the system. Figure 14b  
11 is an example of a main menu 854 offering many additional features and submenus 858  
12 to the subscriber. For example, Figure 14b shows that the viewer 266 is able to choose  
13 by a point and click method, many options including: (1) free previews, (2) books you  
14 can order, (3) books in your library, (4) your current book, (5) help, (6) on-line services  
15 and (6) other system features. Following a selection on the main menu 854, a  
16 corresponding submenu 858 is shown.

17 Figure 13 shows fourteen available primary or first level submenus. They are (1)  
18 account set up 862, (2) free previews 866, (3) book suggestion entries 855, (4) books in  
19 your library 872, (5) books you can order 878, (6) your current book 884, (7) help 887,  
20 (8) available features 890, (9) messages 893, (10) account information 896, (11) outgoing  
21 message submenu 898, (12) show links submenu 970, (13) create links submenu 980, and  
22 (14) show interactive files submenu 990. Figure 14c is an example of a first level  
23 submenu for books in your library 872. This "Book In Your Library" example submenu  
24 872 shows six available books by title and author and provides the subscriber with the  
25 ability to check a different shelf of books 874 or return to the main menu 854. Figures  
26 14d and 14e show example submenus 858 for books that may be ordered using the  
27 "Books You Can Order" submenu 878.



Figure 14f is an example of a confirmation menu which confirms a subscribers order. In this particular example, the subscriber is required to enter a PIN number to complete the subscriber's order. Any alpha-numeric or similar password may be used to ensure the subscriber is an authorized subscriber. In one embodiment, the subscriber confirms an order with a PIN or password and then receives a final confirmation screen. The final confirmation screen is primarily text and may state:

**Your book order is now being processed using CABLE.**

**Your book will be delivered overnight and your VISA account will be charged \$2.95.**

**Your book will be available for reading at 6:00AM EST tomorrow. Make sure that:**

- 1. your Library Unit and Cable Connection Unit are plugged in with aerials up tonight; and**
- 2. you tune your cable converter to THE BOOK Channel. The TV set does not have to remain on.**

or similar language.

Examples of the "Account Set Up Menu" 862 and further submenus 858 related to account set up (which provide instructions and account input 864) are shown in Figures 14g and Figure 14h. These submenus 858 allow initialization of an account at the operations center 250 and orders to be charged to credit cards. The submenus 858 include the ability to enter data related to your desired PIN number or password, credit cards, phone numbers, etc. In one embodiment, the account set up is performed using the telephone system. A confirmation menu verifies that the account has been properly set up with the desired PIN or password and credit card. However, additional set-up methods are presented in the referenced related applications.

Free previews for books 866 are also provided by submenus (868, 870). Examples of the free preview menus are shown in Figure 14i and Figure 14j. Figure 14i shows a menu depicting various books for which previews are available for viewing. Following a book selection, a screen submenu showing an excerpt of the selected book cover's description is provided along with an excerpt from a critic's review of the selected book. In one embodiment, this preview screen for a particular book also allows the

1 subscriber to select a submenu, which provides information about the author. The book  
2 preview submenu may also include a still video picture or graphics portraying a book  
3 cover or a scene from the book. An example of such a still video picture or graphics is  
4 shown in figure 14j, which depicts a preview screen 870 about the author. The author's  
5 preview screen 870 shows a picture of the author, provides a short biography, and may  
6 allow the subscriber to order the author's books. The price for ordering the authors  
7 various books may also be shown on the menu.

8 In addition to free previews, in other embodiments, the electronic book system  
9 200 provides the subscriber with a book suggestion feature (see 855). This is  
10 accomplished using the menu system 851 and the processor with associated memory  
11 located at the viewer 266, library 262 or at the distribution point (1020 or 250). When  
12 necessary, information for the book suggestion feature is sent in the text data of the signal  
13 to the home system 258. With this feature, books or authors are suggested to a subscriber  
14 based upon historical data of the subscriber's previous orders, demographics or mood of  
15 the subscriber, other indicators, and/or by text word searches.

16 In one book suggestion embodiment, text word searches of preview information  
17 (such as book cover descriptions, critics reviews and biographies about the author) and/or  
18 text of books or other titles are performed by the library 262 using databases stored in the  
19 library memory 600. Personalized book or author suggestions are made to the subscriber  
20 by obtaining information from the subscriber indicative of general subscriber interests.  
21 Subscriber entries may be solicited from the subscriber using the book suggestion entry  
22 submenu 855. The system uses these subscriber entries either directly or indirectly to  
23 search for books or authors to suggest to the subscriber.

24 Generally, the electronic book suggestion methods may be categorized into two  
25 categories, either responsive methods (which respond to a series of subscriber menu  
26 entries), or intelligent methods (which analyze data to suggest a book). Using a  
27 responsive or intelligent method, the system 200 determines a list of suggested titles or

1 authors and creates a second or third level submenu 856, 857 to suggest the titles for  
2 subscriber selection.

3 Responsive methods of suggesting titles include, for example, the use of mood  
4 questions, searching for authors, and keyword searching. Using the instruction memory  
5 732 and menu generation hardware (e.g., 607) of the viewer 266, a series of mood  
6 questions can be presented on menus to determine a subscribers interest at a particular  
7 time. For this methodology, the home system's 250 processor 404 and instruction  
8 memory 416 assign each title mood indicators (and sub-indicators) from a group such as  
9 light, serious, violent, short, long, dull, exciting, complex, easy-read, young theme, old  
10 theme, adventure, romance, drama, fiction, science-fiction, etc. These indicators are sent  
11 to the home system 258 with the text data and are stored in library memory 600. Based  
12 upon the subscriber entries, the processor associates a set of indicators with the  
13 subscriber's request and a set of books with matching indicators are located for suggesting  
14 to the subscriber.

15 Responsive searches for authors or keywords (a search word provided by the  
16 subscriber) are generally performed by the library processor 628 and instruction memory  
17 632 on data stored in the library memory 600. For example, a keyword given by the  
18 subscriber may be searched for a match in library memory 600 storing the book reviews,  
19 critics and previews databases. Thus, if a subscriber provided an entry of the word  
20 "submarine" on an appropriate submenu, the title "Hunt For Red October" may be  
21 located by the microprocessor 628 using instruction from a routine in instruction memory  
22 632.

23 Intelligent methods of suggesting programs include analyzing personal profile  
24 data on the subscriber and/or historical data about the subscriber such as past books  
25 ordered by the subscriber (or buy data). This method may be performed at the  
26 distribution point or operations center 250 by the on-site processor 404 using subscriber  
27 databases stored in memory 428. The home system 258 receives the text data including  
28 program suggestion information from the distribution point or operations center 250 and

1 generates the program suggestion submenus 855, 856, 857 using the same text data  
2 receiving 212 and viewer menu generation hardware (e.g., 607, 621) described above.  
3 Software routines and algorithms stored in instruction memories (e.g. 632, 732) are used  
4 to analyze historical data and book ordered data to determine a line of books to suggest  
5 to the subscriber.

6 The algorithms for this powerful feature of suggesting books or authors to  
7 subscribers is disclosed in great detail in U.S. Patent Number 5,798,785, entitled  
8 **TERMINAL FOR SUGGESTING PROGRAMS OFFERED ON A TELEVISION**  
9 **PROGRAM DELIVERY SYSTEM**, filed December 2, 1993, which is incorporated  
10 herein by reference.

11 Referring to Figure 13, submenus 858 are shown on the "Books In Your Library"  
12 submenu 872 and may be broken into shelf numbers with submenus for each shelf 874,  
13 876. The submenus 858 for the "Books You Can Order" submenu 878 is similarly  
14 broken out into submenus by shelves 880, 882. These shelves may each be a category or  
15 genre of books. Books may be grouped into categories such as best sellers, novels,  
16 fiction, romance, etc. See Figure 14d.

17 Referring to Figure 13, the submenu 858 for "Your Current Book" 884 allows a  
18 subscriber to select a current book 884 and then determine what page to view. This  
19 selection is confirmed with a level two submenu 885. The help submenu 887 provides  
20 the subscriber with additional help screens 888. The submenus 858 for available features  
21 890 may be broken out into a sequence of separate submenus for each feature 891, 892.  
22 Referring to Figure 13, messages can also be sent with the electronic book selection and  
23 delivery system 200. A level one message screen provides the subscriber with the ability  
24 to select from various messages the subscriber has pending 893. Each message is then  
25 shown on a separate submenu screen 894, 895. The message may contain text and  
26 graphics.

27 Referring to Figure 13, account information is shown on a level one submenu 896  
28 and then follow-on submenus 858 show the recent orders and your account balance 897.

1 There is also a level one submenu for outgoing messages 898 which has a follow-on  
2 submenu used as an input screen 899.

3 In addition to the specific features and submenus described in Figure 13 and  
4 Figure 14a through Figure 14j, many other variations and features are possible. When  
5 a book is finally selected for viewing the title page 886 will appear on the screen followed  
6 by a page of text.

### 7 III. The Billing And Collection System

8 In one embodiment, the billing and collection system 278 (shown in Figures 2 and  
9 3) utilizes the latest technology in electronic transaction and telephone switching to track  
10 orders, authorize deliveries, bill consumers, and credit publishers automatically. The  
11 telephone calls initiated by the phone connector 270 are received by the billing and  
12 collection system 278 which responds immediately without human intervention by  
13 placing the order and charging the consumers credit card account. Data is compiled  
14 periodically and publishers 282 are credited for sales of their books or other text. The  
15 billing and collection system 278 may also connect with subscribers through two-way  
16 cable connections, cellular, or other communication means. These additional methods  
17 are detailed in the referenced related applications.

18 The billing and collection system 278 communicates with the operations center  
19 to track changes in available books and to provide statistical data to the operations center  
20 250.

### 21 IV. Public Library, School, and Bookstore System

22 The electronic book system can be modified to be used at public libraries, schools,  
23 bookstores, newsstands, or stand-alone kiosks. Figure 15 shows one possible  
24 arrangement of components for the distribution location. The main unit is the file server  
25 900. The file server 900 is a large electronic memory unit that can store thousands of  
26 books, newspapers, or periodicals. Various electronic storage means may be used in the  
27 file servers, such as hard disks, read-write CD ROMs and read-only CD ROMs.

The system comprises five components; the file server 900, a converter or video connector 904 or connector capable of interfacing to one of the alternative delivery systems presented in the referenced related applications, a controller 908, a viewer 912, and a catalog printer 916. The software for controlling the system is primarily located in the controller 908. The converter or video connector 904 is similar to those described above. In this configuration the controller unit 908 monitors the data being transferred to the file server 900 by the converter 904. The controller 908 may be provided with a viewing screen and several control buttons. When it is necessary to have a larger screen to perform more sophisticated controlling of the system a viewer 266 may be connected to the controller 908 and the viewer screen and controls 740 may be used.

For security reasons, the controller 908 is only able to download books to public viewers 912 which are authorized to receive books from the particular file server 900. Also for security reasons it is not desirable that the public viewer 912 have access to more than one file server 900. In this way, security can be maintained over the text data for books. The public viewer 912 may be limited to receiving one or two books at a time from the controller 908. When the user of the public viewer 912 needs a new or additional book, the user returns the viewer 912 to the school or public library where the user receives a new book from the controller 908. Additional security mechanisms associated with this kiosk-based distribution of electronic books are presented in Section VII.

In order to track the books that are available on the file server 900, the titles of the available books may be printed on a catalog printer 916. The catalog printer 916 is connected to the library controller 908 and the titles of the books are downloaded to the catalog printer 916. For security reasons, the coded text for any of the electronic books may not be authorized for printing using the controller 908 and catalog printer 916. In order to maintain security over the data, none of the electronic book data may be allowed to be downloaded to the printer 916. Once a complete printout of available book titles,

1 magazines, or other textual material is complete, a hard copy of the catalog 920 can be  
2 maintained at the file server 900.

3 The system shown may also be used at bookstores. The bookstores can rent the  
4 public viewer 912 to customers with the text for one or two books loaded onto the public  
5 viewer 912. The public viewer 912 may be provided with an automatic timeout  
6 sequence. The timeout sequence would erase the textual data for the books after a certain  
7 period of time, for example, two weeks. It is expected that after a period of time (perhaps  
8 within two weeks) the renter would return the public viewer 912 to the bookstore and  
9 receive additional books for viewing. Using this arrangement, it is also possible for the  
10 bookstore to (permanently) sell a viewer 912 to a regular customer. The customer then  
11 returns to the bookstore from time to time to receive textual data for a book which the  
12 customer can then store permanently on the customer's own viewer 912. Various other  
13 configurations are possible for bookstores, schools and public libraries using the file  
14 server 900 and public viewer 912 can be described.

#### 15 V. Use of A Set Top Converter

16 Existing set top converter boxes such as those made by Scientific Atlanta or  
17 General Instruments are presently unequipped to handle the book selection system of the  
18 present invention. Although set top converters may be built which include the library  
19 functions, hardware modifications are necessary in order to use the book selection system  
20 with existing set top converter technology.

21 Figures 16a and 16b are examples of hardware modifications or upgrades. A port  
22 is used to attach hardware upgrades described below to a set top terminal. Two upgrades  
23 are possible to set top converters 601 to assist in receiving and selecting electronic books,  
24 a menu generation card upgrade (Figure 16a) and an information download unit (Figure  
25 16b). Each of these upgrades may be connected to the set top terminal unit through an  
26 upgrade port. A four wire cable, ribbon cable, FireWire (IEEE 1394B) interface  
27 connector, USB connector, or the like may be used to connect the upgrade to the set top  
28 converter 601.

1 A card addition 950 to a set top converter 601 is depicted in Figure 16a. The card  
2 950 shown provides the additional functionality needed to utilize the book selection  
3 system with existing set top converter 601 technology. The card 950 may be configured  
4 to slip inside the frame of a set top terminal and become part of the set top terminal, an  
5 advanced set top terminal. The primary functions the card 950 adds to the set top  
6 converter 601 are the interpreting of data signals, generating of menus, sequencing of  
7 menus, and, ultimately, the ability of the subscriber to select a book using either the  
8 television or a viewer 266. The card 950 also provides a method for a remote location,  
9 such as the cable headend, to receive information on books ordered. The books ordered  
10 information and control commands may be passed from the cable headend to the card 950  
11 using telephone lines or alternative ordering methods as presented in the referenced  
12 related applications.

13 The primary components of the card 950 are a PC chip CPU 952, a VGA graphic  
14 controller 954, a video combiner 956, logic circuitry 958, NTSC encoder 960, a receiver  
15 962, demodulator (not shown), and a connector 611', which consists of a dialer. The card  
16 950 operates by receiving the data text signal from the cable headend through the coaxial  
17 cable. The logic circuitry 958 of the card 950 receives data 964, infrared commands 966,  
18 and synchronization signals (not shown) from the set top converter 601. Menu selections  
19 made by the viewer 266 on the remote control are received by the set top converter's 601  
20 IR equipment and passed through to the card 950. The card 950 interprets the IR signal  
21 and determines the book (or menu) the subscriber has selected. The card 950 modifies  
22 the IR command to send the information to the set top converter 601. The modified IR  
23 command contains the channel information needed by the set top converter 601. Using  
24 the phone line 968 and dialer 611', the card 950 is able to transmit electronic books  
25 ordered information to the cable headend. It is also possible to receive the electronic  
26 books over the telephone lines and other telecommunications networks, including  
27 wireless networks, and by-pass the video distribution system.



1           These commands are passed through the interface linking the set top terminal's  
2           microprocessor with the microprocessor of the hardware upgrades. In this way,  
3           subscriber inputs, entered through the set top terminal keypad or remote control, can be  
4           transferred to any of the hardware upgrades for processing and responses generated  
5           therein can then be sent back to the set top terminal for display. In one embodiment the  
6           IR commands 966 are transferred from set top terminal 601 to hardware upgrade.

7           Hardware upgrades may include a microprocessor, interactive software,  
8           processing circuitry, bubble memory, and a long-term memory device. In addition to  
9           these basic components, the hardware upgrade may make use of an additional telephone  
10          modem or CD-ROM device.

11          An information download hardware upgrade 1001 shown in Figure 16b allows the  
12          subscriber to download large volumes of information from the operations center 250 or  
13          cable headend using a set top terminal 610. The hardware upgrade 1001 will enable  
14          subscribers to download data, such as electronic books and electronic magazines, to local  
15          secure storage. Primarily, the hardware upgrade 1001 is an additional local storage unit  
16          1003 (e.g., hard disk, floppy, optical disk or magnetic cartridge and may include a  
17          microprocessor 1005, instruction memory 1007, and a random access memory 1009, as  
18          shown in Figure 16b). A small portable viewer may also provided with the upgrade 1001  
19          to enable downloaded text to be read without the use of a television.

20          The downloadable information may be text or graphics supplied by the operations  
21          center 250 or cable headend. With the upgrade 1001, electronic books may be  
22          downloaded and read anywhere with the viewer 266. Using the upgrade 1001, electronic  
23          books may be downloaded and stored in compressed form for later decompression. The  
24          electronic books may be decompressed only at the time of viewing. Important text that  
25          the public desires immediate access may made available through this system. Text such  
26          as the President's speech, a new law, or a recent abortion decision rendered by the  
27          Supreme Court may be made immediately available.

In one embodiment, electronic book ordering information is stored at each set top terminal 610 until it is polled by the cable headend using a polling request message format. An example of a polling request message format consists of six fields, namely: (1) a leading flag at the beginning of the message, (2) an address field, (3) a subscriber region designation, (4) a set top terminal identifier that includes a polling command/response (or P/F) bit, (5) an information field, and (6) a trailing flag at the end of the message. A similar response frame format for information communicated by the set top terminal to the cable headend in response to the polling request may be used.

Figure 17 shows components of a set top terminal 610'. The components include a data receiver 617' and a data transmitter 1011. The data transmitter provides upstream data communications capability between the set top terminal 610' and the cable headend. Upstream data transmissions are accomplished using the polling system described and, using a data transmitter 1011. Both receiver 617' and transmitter 1011 may be built into the set top terminal 610' itself or added through an upgrade module. Regardless of the specific hardware configuration, the set top terminal's data transmission capabilities may be accomplished using the hardware shown in Figure 17.

Figure 17 shows RF signals, depicted as being received by a data receiver 617' and tuner 613 working in unison. Both of these devices are interfaced with the microprocessor 1013, which receives inputs 1015, from the subscriber, either through a set top terminal's keypad, a remote control unit or viewer 266. Generally, all cable signals intended for reception on the subscriber's TV are accessed by the tuner 613 and subsequently processed by the processing circuitry 1017. This processing circuitry 1017 typically includes additional components (not shown) for descrambling, demodulation, volume control and remodulation on a Channel 3 or 4 TV carrier.

Data targeted to individual set top terminals is received by the data receiver 617' according to each set top terminal's specific address or ID. In this way, each addressable set top terminal 610' only receives its own data. The data receiver 617' may receive set

1 top terminal 610' specific data in the information field of the signal frame described or  
2 on a separate data carrier located at a convenient frequency in the incoming spectrum.  
3 The received data includes information regarding electronic books and menus available  
4 for selection. The subscriber may enter a series of commands 1015 using a keypad or  
5 remote control in order to choose an electronic book or menu. Upon receipt of such  
6 commands, the set top terminal's microprocessor 1013 instructs the tuner to tune to the  
7 proper frequency of the channel carrying data and subsequently instructs the processing  
8 circuitry 1017 to begin descrambling of this data.

9 Upon selection of an electronic book, the microprocessor 1013 stores any  
10 selection information in local memory (not shown) for later data transmission back to the  
11 cable headend. The set top terminal's microprocessor 1013 coordinates all CATV signal  
12 reception and also interacts with various upstream data transmission components.  
13 Typically, the data transmitter 1011 operates in the return frequency band between 5 and  
14 30 MHZ. In an alternative embodiment, the frequency band of 10 to 15 MHZ may be  
15 used. Regardless, however, of the frequency band used, the data transmitter 1011 sends  
16 information to the cable headend in the information field of the response frame described.  
17 Those skilled in the art will recognize that a number of variations and combinations of  
18 the above-described set top terminal hardware components may be used to accomplish  
19 upstream data transmissions.

## 20 VI. Books-On-Demand System

21 The electronic book system 200 described may also be configured in a  
22 book-on-demand style. Figure 18a shows one example of a configuration for a  
23 book-on-demand system. A book on demand system requires more powerful two-way  
24 communications between the consumer's home, bookstore, school or public library and  
25 either the operations center 250 or a distribution site 1020 such as the cable headend. In  
26 one embodiment, this type of two-way communication can be provided by the hardware  
27 shown in Figure 17 and described above. Additional methods related to alternative  
28 communication paths are presented in the referenced related applications.

Referring to Figure 18a, in a book-on-demand system, the subscriber selects the book to be download from an available menu of books (see for example Figures 14d and 14e). The data for menus of available books is usually sent to the subscriber location by the distribution site 1020. After the subscriber's menu selection, information about the subscriber selection (or request) is then communicated to either a distribution point 1020 (such as a cable headend) or the operations center 250. Upon receipt of this request, the needed textual and graphical information for the book is spooled and sent to the subscriber. In this manner, electronic books are only sent when requested by the subscriber and are sent immediately upon demand for the electronic book (or text).

In order to support such a demand system, the text delivery and distribution must be conducted on a strong nodal architecture distribution system, such as, a video-on-demand cable or telephone television system, through use of individual telephone calls on the public telephone system or cellular phone system, through the use of the Internet, or a number of other data network options.

The book-on-demand system allows for a greater selection of electronic books to the subscriber and limits the amount of communicated book data that is unnecessary or unneeded. It also provides the electronic book to the subscriber in a much timelier fashion.

In addition to a stronger distribution system, a book-on-demand system requires a distribution point 1020 to have more sophisticated equipment to access and "spool out" the textual information. This can be accomplished using file server technology 1024 for storing the books and distribution technology such as ATM 1028 or telephone-type switching (not shown) to distribute the textual information. The file server 1024 and distribution technology that can be used in configuring such a book-on-demand system is described in U.S. Patent No. 5,262,875 and U.S. Patent 5,218,695, cited above.

Figure 18a shows an embodiment for a book-on-demand system that utilizes file server technology. In addition to books, the embodiment of Figure 18a will support distribution of nearly any digital data. Books or textual files are received from publishers

1 282 and other sources through local feeds 1032, ATM 1028, or by satellite dish 1036, for  
2 example. The data is then stored in memory 1040 at the file server 1024. In one  
3 embodiment, the distribution point 1020 is a cable headend that receives requests from  
4 subscribers and delivers text to subscribers over a two-way communication system (such  
5 as a video-on-demand system (VOD) 1044).

6 The library 262 can be connected to either a basic premium-type service cable  
7 system 1048, a near video-on-demand type cable system (or pay-per-view (PPV) 1052)  
8 or a video-on-demand cable system 1044. In connecting with either of these three  
9 systems the library 262 may access the cable directly or may access the system through  
10 a set top terminal 601', 601", or 601'''.

11 Using the two-way video-on-demand system 1044, a subscriber is able to request  
12 a specific book title and receive that text immediately following its request. To  
13 accomplish this, the distribution point 1020 transmits a list of available books through  
14 the cable delivery system to the library 262. The library 262 displays the list of available  
15 books on a menu or similar format. As described earlier, the library 262 may use menus  
16 which list categories of available books to form its request from the distribution point  
17 1020. After selecting a book the library 262 then sends a request signal on the two-way  
18 communication system 1044 back to the distribution point 1020. This request signal can  
19 be handled in two ways. The library 262 either initiates the request or the distribution  
20 point 1020 polls the various libraries on to the two-way system 1044. Upon receiving the  
21 request for the book title, the text associated with that book title is transmitted to the  
22 library 262 using the two-way cable system 1044.

23 Figure 18b is an expanded view of an operations center 250 that supports a  
24 regional or national book-on-demand system. In fact, the operations center 250 shown  
25 supports distribution of nearly any digital data. The operations center 250 supports  
26 multiple feeds to receive digital information by tape 1060, 1060', ATM 1028, or satellite  
27 1036. The information is processed through an input MUX 1064 and a small file server  
28 1068 before reaching the master file server 1072. Digital data such as books received

from publishers 282 is then stored on the master file server 1072. The digital data may be stored compressed in a standard format such as MPEG2.

A system controller 1076 provides control over the regional or national book-on-demand system. Books may be packaged into groups to provide feeds to various cable headends. In addition, scheduling and marketing research are conducted at the operations center 250. In order to handle the scheduling and market research, book buy data is received at the operations center 250 through a multiplexer 1082. Book buy information can be provided by the operations center 250 to the billing and collection system 278.

The operations center 250 is also equipped to insert messages or advertisements into the file server. These messages or advertisements will eventually be received by the subscribers.

The master file server 1072 uses an output multiplexer 1080 and ATM 1028 as well as satellite connections to distribute digital data. In one embodiment, cable headends receive text data on books from the master file server 1080 through the output multiplexer 1028 and an ATM system 1028. After receiving the digital book data, the cable headends store the books in a local file server 1024. Figure 18a's distribution point 1020 is an example of a cable headend which may receive data from the operations center 250 of Figure 18b through an ATM hookup 1088 or satellite hookup. All communications and storage in the Book on Demand system may make use of the security mechanisms presented in Section VII.

## VII. Electronic Book Security Mechanisms

The electronic book distribution system and components may incorporate various forms of security using cryptographic mechanisms. Cryptography consists of an encryption and reversing decryption process. A basic encryption process operates on a string of digital bits, or clear text, by modifying the clear text using a series of mathematical operations with both the clear text and a second string of bits, called an encryption key, as inputs, resulting in a third string of bits, called ciphertext. A reversing

process exists using a fourth string of bits, called a decryption key, that, when input into a decryption process consisting of a second series of mathematical operations, along with the ciphertext, the resulting output is the original clear text string of digital bits.

Two types of techniques underlie the majority of encryption mechanisms associated with electronic book security: symmetric encryption and asymmetric public key encryption. Referring to Figure 19a, symmetric encryption uses a cryptographic algorithm where the same key used by encryption process 5001 to encrypt data is also used by decryption process 5002 to decrypt data. Henceforth, for uses of symmetric key encryption, encryption of unencrypted content X 5003, using symmetric key SK 5004 is represented as  $E_{SK}[X]$  5005, whereas decryption of encrypted content  $E_{SK}[X]$  5005 using symmetric key SK 5004, is represented as  $D_{SK}[E_{SK}[X]]$  and results in unencrypted content X 5003.

Asymmetric public key encryption is a cryptographic system using two keys, one key to encrypt content, and a different key to decrypt the same content. These key pairs and the associated cryptographic algorithms are constructed such that knowledge of one of the two keys does not reveal the other key. Additionally, in asymmetric public key encryption, content encrypted using one key cannot be decrypted using the same key. Therefore, one of the keys of the key pair, the public key, can be distributed widely, while the other key of the key pair is held closely and protected, the private key. This allows a first party, or a sender S to encrypt content using the sender's private key, pKS 5013 and encryption process  $E_{pKS}$  5011. The sender can then distribute the resulting encrypted content  $E_{pKS}[X]$  5014 to any second party, or recipient that possesses the sender's public key PKS 5015. The recipient can then decrypt the encrypted content  $E_{pKS}[X]$  5014 using the sender's public key, PKS 5015 and decryption process  $D_{pKS}$  5012. Encryption of unencrypted content X 5003 using the private key of sender S is represented as  $E_{pKS}[X]$ , whereas decryption of the encrypted content, using the public key of the sender is represented as  $D_{pKS}[E_{pKS}[X]]$ . Figure 19b depicts the case where content is encrypted in a private key. Alternatively, the sender could use the recipient public key PKR 5023 and

1 encryption process  $E_{PKR}$  5021 to encrypt the unencrypted content X 5003. Then, only the  
 2 recipient, using a recipient's private key  $pKR$  5025, is able to decrypt the encrypted  
 3 content  $E_{PKR}[X]$  5024 using decryption process  $D_{pKR}$  5022. Encryption of the unencrypted  
 4 content X 5003 using the recipient's public key  $PKR$  5025, is represented as  $E_{PKR}[X]$ ,  
 5 whereas decryption of the encrypted content  $E_{pKS}[X]$  5014, using the recipient's private  
 6 key 5025 is represented as  $D_{pKR}[E_{PKR}[X]]$ . Figure 19c depicts the case where content is  
 7 encrypted in a public key.

#### 8 A. Publisher to Operations Center Communications Security

9 Publishers 282 or other content providers 110 can deliver their electronic book  
 10 content to the operations center 250 via a secured mechanism. In one embodiment, an  
 11 asymmetric public key encryption technique is used, as described in Contemporary  
 12 Cryptography, edited by Gustavus Simmons, published by IEEE Press in 1992, and  
 13 hereby incorporated by reference. Public key algorithms used may include the  
 14 Merkle-Hellman Knapsacks technique, as described in U.S. Patent 4,218,582 to Hellman  
 15 and Merkle, the RSA technique, as described in U.S. Patent 4,405,829 to Rivest, Shamir,  
 16 and Adleman, the Pohlig-Hellman technique, as described in U.S. Patent 4,424,414 to  
 17 Hellman and Pohlig, the Schnorr Signatures technique, as described in U.S. Patent  
 18 4,995,082 to Schnorr, or any comparable public key technique. The techniques described  
 19 in these U.S. Patents are hereby incorporated by reference. In an embodiment depicted  
 20 in Figure 20, a publisher 282, serving as a sender 4998, first encrypts electronic book  
 21 content EBC 5100 destined for the operations center 250, which serves as the recipient  
 22 4999, using a symmetric key encryption process  $E_{SK}$  5102 and DES, PKZIP, BLOWFISH,  
 23 or any other symmetric encryption algorithm, resulting in encrypted content  $E_{SK}[EBC]$   
 24 5109. The encryption process  $E_{SK}$  5102 uses a symmetric key SK 5103 either randomly  
 25 generated by a key generator process 5104 or previously defined and retrieved from key  
 26 storage memory 5105. Then, the publisher 282 encrypts the symmetric key SK 5103 with  
 27 private key encryption process  $E_{pKS}$  5106 using the publisher's private key  $pKS$  5107,  
 28 resulting in encrypted key  $E_{pKS}[SK]$  5108. Then, the publisher 282 packages encrypted



key  $E_{PKS}[SK]$  5108, encrypted content  $E_{SK}[EBC]$  5109 and non-encrypted information 5110 related to the electronic book or the exchange and delivers the package to the operations center 250. Using decryption process  $D_{PKS}$  5111 and the publisher's public key  $PKS$  5112, the operations center 250 decrypts the encrypted key  $E_{PKS}[SK]$  5108 and uses the recovered symmetric key  $SK$  5103 to decrypt the encrypted content  $E_{SK}[EBC]$  5109 using decryption process  $D_{SK}$  5113.

In an alternate embodiment, depicted in Figure 21, symmetric key encryption is used in conjunction with a certificate authority 4997. The certificate authority 4997, a trusted source, provides a symmetric key to each publisher 282, serving as the sender 4998, and the operations center 250, serving as the recipient 4999. The certificate authority 4997 may be an existing commercial entity such as Entrust or Verisign or a private entity established for the sole purpose of electronic book secure distribution. The publisher 282 contacts the certificate authority 4997, sending a request 5120 for a transaction symmetric key  $SKT$  5121 to be used during a transaction. The certificate authority 4997 either randomly generates the transaction symmetric key  $SKT$  5121 by using a key generator process 5124 or retrieves the previously defined transaction symmetric key  $SKT$  5121 from key storage memory 5125. The transaction symmetric key  $SKT$  5121 is encrypted by the certificate authority 4997 using symmetric key encryption process  $E_{SKS}$  5123 and the publisher's symmetric key  $SKS$  5122. A resulting encrypted transaction symmetric key  $E_{SKS}[SKT]$  5126 is delivered by the certificate authority 4997 to the publisher 282. The publisher 282 decrypts the encrypted transaction symmetric key  $E_{SKS}[SKT]$  5126 using decryption process  $D_{SKS}$  5127 and the publisher's symmetric key  $SKS$  5122 to recover the transaction symmetric key  $SKT$  5121. The publisher 282 then uses the recovered transaction symmetric key  $SKT$  5121 received from the certificate authority 4997 to encrypt the electronic book content  $EBC$  5100 using encryption process  $E_{SKT}$  5128, resulting in encrypted content  $E_{SKT}[EBC]$  5129. The publisher 282 then delivers the encrypted content  $E_{SKT}[EBC]$  5129 to the operations center 250. The transaction symmetric key  $SKT$  5121 is also encrypted by the certificate

1 authority 4997 using symmetric key encryption process  $E_{SKR}$  5131 and the operations  
 2 center's symmetric key SKR 5130. The resulting encrypted transaction symmetric key  
 3  $E_{SKR}[SKT]$  5132 is delivered by the certificate authority 4997 to the operations center  
 4 250. The operations center 250 decrypts the encrypted transaction symmetric key  
 5  $E_{SKR}[SKT]$  5132 using decryption process  $D_{SKR}$  5133 and the operations center's  
 6 symmetric key SKR 5130 to recover the transaction symmetric key SKT 5121. The  
 7 operations center 250 then uses the recovered transaction symmetric key SKT 5121  
 8 received from the certificate authority 4997 to decrypt the encrypted content  $E_{SKT}[EBC]$   
 9 5129 using decryption process  $D_{SKT}$  5134, resulting in unencrypted electronic book  
 10 content 5100.

11 In yet another embodiment, depicted in Figure 22, the publisher 282, acting as the  
 12 sender 4998, generates a transaction symmetric key SKT 5140. The publisher 282 either  
 13 randomly generates the transaction symmetric key SKT 5140 by using a key generator  
 14 process 5141, or retrieves a previously defined transaction symmetric key SKT 5140 from  
 15 key storage memory 5142. The publisher 282 encrypts the electronic book content EBC  
 16 5100 using encryption process  $E_{SKT}$  5143 and the transaction symmetric key SKT 5140,  
 17 and delivers encrypted content  $E_{SKT}[EBC]$  5144 to the operations center 250, acting as  
 18 recipient 4999. The publisher 282 then encrypts the transaction symmetric key SKT 5140  
 19 using encryption process  $E_{SKS}$  5145 and a publisher's symmetric key SKS 5146 that it  
 20 shares with a third party certificate authority 4997 and delivers an encrypted symmetric  
 21 key  $E_{SKS}[SKT]$  5147 to the certificate authority 4997. The certificate authority 4997  
 22 decrypts the encrypted symmetric key  $E_{SKS}[SKT]$  5147 using decryption process  $D_{SKS}$   
 23 5148 and the publisher's symmetric key SKS 5146. The operations center 250 may  
 24 contact the certificate authority 4997 using request 5149 to obtain the transaction  
 25 symmetric key SKT 5140. Prior to the certificate authority 4997 delivering the needed  
 26 transaction symmetric key 5140 to the operations center 250, the operations center 250  
 27 may be required to complete a financial transaction with the certificate authority 4997,  
 28 paying for the electronic book content first. The certificate authority 4997 then encrypts

1 the transaction symmetric key SKT 5140 using encryption process  $E_{SKR}$  5150 and an  
 2 operations center's symmetric key SKR 5151 that the certificate authority 4997 shares  
 3 with the operations center 250 and delivers encrypted symmetric key  $E_{SKR}[SKT]$  5152 to  
 4 the operations center 250. The operations center 250 decrypts the encrypted symmetric  
 5 key  $E_{SKR}[SKT]$  5152 using decryption process  $D_{SKR}$  5153 and the operations center's  
 6 symmetric key SKR 5151, and uses the recovered transaction symmetric key SKT 5140  
 7 to decrypt the encrypted content  $E_{SKT}[EBC]$  5144 using decryption process  $D_{SKT}$  5154,  
 8 resulting in electronic book content EBC 5100.

9 In another embodiment, depicted in Figure 23a, the publisher 282, serving as the  
 10 sender 4998, encrypts a transaction stream TS 5165 between the publisher 282 and the  
 11 operations center 250, serving as the recipient 4999. To do so, the publisher 282 may use  
 12 a sender private key  $pKS$  5160 and encryption process  $E_{pKS}$  5161 to encrypt the  
 13 transaction stream TS 5165, resulting in encrypted transaction stream  $E_{pKS}[TS]$  5162.

14 In this embodiment, the operations center 250 uses decryption process  $D_{pKS}$  5164  
 15 and sender public key  $PKS$  5163 to decrypt the encrypted transaction stream  $E_{pKS}[TS]$   
 16 5162. In another embodiment, depicted in Figure 23b, the publisher 282, serving as the  
 17 sender 4998, may use a public key of the operations center 250, serving as the recipient  
 18 4999, to encrypt the transaction stream TS 5165. To do so, the publisher 282 may use  
 19 a recipient public key  $PKR$  5171 and encryption process  $E_{PKR}$  5170 to encrypt the  
 20 transaction stream TS 5165, resulting in encrypted transaction stream  $E_{PKR}[TS]$  5173.

21 In this embodiment, the operations center 250 uses decryption process  $D_{pKR}$  5174  
 22 and recipient private key  $pKR$  5172 to decrypt the encrypted transaction stream  $E_{pKR}[TS]$   
 23 5173. In another embodiment, depicted in Figure 23c, the publisher 282, serving as the  
 24 sender 4998, may use a transaction symmetric key SKT 5181 that both the publisher 282  
 25 and the operations center 250 have stored in advance of the transaction to encrypt the  
 26 transaction stream TS 5165. In this embodiment, the publisher 282 uses encryption  
 27 process  $E_{SKT}$  5180 and transaction symmetric key SKT 5181 to generate the encrypted  
 28 transaction stream  $E_{SKT}[TS]$  5182. The operations center 250 uses decryption process

1  $D_{SKT}$  5183 and transaction symmetric key SKT 5181 to decrypt the encrypted transaction  
2 stream  $E_{SKT}[TS]$  5182, resulting in the transaction stream TS 5165.

3 In another embodiment, depicted in Figure 24a, the publisher 282, serving as the  
4 sender 4998, and the operations center 250, serving as the recipient 4999, initiate the  
5 transaction by negotiating a shared key to use for the transaction, using, for example, the  
6 Elliptic Curve Diffie-Hellman key exchange algorithm, described in U.S. Patent  
7 4,200,700 to Hellman, Diffie, and Merkle, which is hereby incorporated by reference, to  
8 generate the shared transaction symmetric key. Key negotiation information 5190 is  
9 exchanged between the publisher 282 and the operations center 250. As a result of the  
10 negotiation process, a publisher's key generator algorithm 5191 generates the transaction  
11 symmetric key SKT 5193 and the operations center's key generator algorithm 5192  
12 generates the transaction symmetric key SKT 5193. The publisher 282 encrypts the  
13 electronic book content EBC 5100 using encryption process  $E_{SKT}$  5194 and the shared  
14 transaction symmetric key SKT 5193 and delivers the resulting encrypted content  
15  $E_{SKT}[EBC]$  5195 to the operations center 250. The operations center 250 uses the shared  
16 transaction symmetric key SKT 5193 and decryption process  $D_{SKT}$  5196 to decrypt  
17 encrypted content  $E_{SKT}[EBC]$  5195. In a different embodiment, depicted in Figure 24b,  
18 the publisher 282 serves as the sender 4998 and operations center 250 serves as the  
19 recipient 4999. Initial key negotiation information 5200 is exchanged between a seed key  
20 generation algorithm 5201 at the publisher 282 and a seed key generation algorithm 5202  
21 at the operations center 250. As a result, the seed key generation algorithm 5201 at the  
22 publisher 282 and the seed key generation algorithm 5202 at the operations center 250  
23 each generate seed key SK 5203 using, for example, the Elliptic Curve Diffie-Hellman  
24 key exchange algorithm, as described in U.S. Patent 4,200,700. The seed key SK 5203  
25 is then used by key sequence generator 5204 at the publisher 282 to generate the first in  
26 a sequence of keys, transaction symmetric key SKTi 5206. Similarly, the seed key SK  
27 5203 is used by key sequence generator 5205 at the operations center 250 to generate an  
28 identical sequence of keys, beginning with shared transaction symmetric key SKTi 5206.

1 The publisher 282 encrypts the electronic book content EBC 5100 using encryption  
 2 process  $E_{SKTi}$  5207 and the shared transaction symmetric key  $SKTi$  5206 and delivers a  
 3 resulting encrypted content  $E_{SKTi}[EBC]$  5208 to the operations center 250. The operations  
 4 center 250 uses the transaction symmetric key  $SKTi$  5206 and decryption process  $D_{SKTi}$   
 5 5209 to decrypt the encrypted content  $E_{SKTi}[EBC]$  5206. The publisher key sequence  
 6 generator 5204 and the operations center key sequence generator 5205 continue to  
 7 generate matching transaction symmetric keys for use in encrypting each subsequent  
 8 transaction between the publisher 282 and the operations center 250.

9 The publisher 282 may deliver the electronic book content to multiple operations  
 10 centers. In one embodiment, the publisher 282 delivers the electronic book content to  
 11 each operations center 250 independently using one of the embodiments described herein.  
 12 In an alternative embodiment, the publisher 282 may broadcast the electronic book  
 13 content to multiple operations centers 250 simultaneously. In one embodiment used for  
 14 broadcasting, depicted in Figure 25a, the publisher 282, serving as the sender 4998,  
 15 encrypts the electronic book content EBC 5100 using encryption process  $E_{SKT}$  5211 and  
 16 transaction symmetric key  $SKT$  5210, resulting in encrypted content  $E_{SKT}[EBC]$  5217.  
 17 The transaction symmetric key  $SKT$  5210 is then encrypted using public key encryption  
 18 process  $E_{PKA}$  5212 and public key  $PKA$  5213 for recipient A 4999, the first operations  
 19 center 250 to receive the electronic book content, resulting in encrypted key  $E_{PKA}[SKT]$   
 20 5218. The transaction symmetric key  $SKT$  5210 is then encrypted using public key  
 21 encryption process  $E_{PKB}$  5212' and public key  $PKB$  5213' for recipient B 4999', the second  
 22 operations center 250 to receive the electronic book content, resulting in encrypted key  
 23  $E_{PKB}[SKT]$  5218'. This process is repeated for each of the operations centers 250  
 24 receiving the electronic book content. The encrypted content  $E_{SKT}[EBC]$  5217, along  
 25 with encrypted keys 5218, 5218', and 5218'', are delivered to all the receiving operations  
 26 centers 250. Each operations center 250 uses its own private key to decrypt the  
 27 transaction symmetric key  $SKT$  5210. For example, recipient A 4999 uses decryption  
 28 process  $D_{pKA}$  5214 and private key  $pKA$  5216 to decrypt the encrypted key  $E_{PKA}[SKT]$

1 5218, recovering the transaction symmetric key SKT 5210. Decryption process  $D_{SKT}$   
2 5215 is then used to decrypt encrypted content  $E_{SKT}[EBC]$  5217 using transaction  
3 symmetric key SKT 5210.

4 In another embodiment, depicted in Figure 25b, operations centers 250 may be  
5 assigned to predefined groups. Prior to the distribution of electronic book content EBC  
6 5100 by publisher 282, serving as the sender 4998, for each defined group, a group  
7 symmetric key SKG 5220 is created and distributed by the publisher 282 to each  
8 operations center 250, serving as recipients 4999, 4999' and 4999" within the group.

9 When the publisher 282 sends the electronic book content EBC 5100 to a  
10 pre-defined group of operations centers, the publisher 282 encrypts the electronic book  
11 content EBC 5100 using encryption process  $E_{SKG}$  5221 and the group symmetric key SKG  
12 5220 pre-defined for that group and delivers the encrypted content  $E_{SKG}[EBC]$  to all the  
13 operations centers 250 in the group. Recipients 4999, 4999', and 4999" use decryption  
14 process  $D_{SKG}$  5223 and the group symmetric key SKG 5220 for that group to which they  
15 are assigned to decrypt the encrypted content  $E_{SKG}[EBC]$ .

16 To ensure that the electronic book content delivered by the publisher 282 to the  
17 operations center 250 was not altered in route, integrity checking algorithms may be  
18 employed. In one embodiment, depicted in Figure 26, the publisher 282, serving as  
19 sender 4998, uses a one-way hashing algorithm 5231, as presented in Applied  
20 Cryptography, by Bruce Schneier, published by John Wiley & Sons, Inc. in 1996, and  
21 hereby incorporated by reference, where a hashing value 5232 is calculated by the  
22 publisher 282 based on the electronic book content file 5230 as an input. This resulting  
23 hashing value 5232, along with the actual encrypted electronic book file 5237 that has  
24 been encrypted by the publisher 282 via encryption process 5235 is delivered to the  
25 operations center 250, serving as the recipient 4999.

26 The operations center 250 decrypts the encrypted electronic book file 5237 using  
27 decryption process 5236 to recover electronic book content file 5230'. The operations  
28 center 250 then uses the hashing algorithm 5231 with the electronic book content file

1 5230' as an input to generate a hashing value 5232'. A comparator 5223 compares the  
2 hashing value 5232' and the hashing value 5232 delivered with the encrypted electronic  
3 book file 5237. If the hashing value 5232' calculated by the operations center 250  
4 coincides with the hashing value 5232 delivered by the publisher 282, the integrity of the  
5 electronic book content file 5230' is ensured.

6 To identify the publisher 282 delivering the electronic book and to guarantee  
7 non-repudiation, i.e., that the publisher 282 cannot deny that the electronic book was sent,  
8 the publisher 282 and operations center 250 may use an authentication method. In one  
9 embodiment, a Digital Signature Algorithm (DSA) is used, as described in U.S. Patent  
10 5,231,668 to Kravitz, and hereby incorporated by reference. In another embodiment, the  
11 publisher 282 uses a password as an identifier. This password may be delivered along  
12 with the electronic book content to authenticate the publisher 282 as the sender. The  
13 operations center 250 compares this password with the password the operations center  
14 250 has for the publisher 282. If the passwords match, the source of the electronic book  
15 content, i.e., the publisher 282, is verified.

16 In yet another embodiment, public key encryption is used as a digital signature to  
17 authenticate the publisher 282. The publisher 282 encrypts the electronic book content  
18 using the publisher's private key pKS. When the operations center 250 correctly decrypts  
19 the encrypted electronic book content with the publisher's public key PKS, the identity  
20 of the publisher 282 is authenticated since only the publisher 282 has access to the  
21 publisher's private key pKS used to encrypt the electronic book content.

22 In another embodiment, depicted in Figure 27, upon initiation of the transaction,  
23 the publisher 282, serving as the sender 4998, notifies the operations center 250, serving  
24 as the recipient 4999, of the publisher's intention to deliver electronic book content to the  
25 operations center 250. This notification may be in the form of delivery notification  
26 message 5240. The operations center 250 then encrypts a randomly generated message  
27 RGM generated by the operations center 250 using encryption process  $E_{pKR}$  and the  
28 operations center's private key pKR and sends the resulting  $E_{pKR}[RGM]$  5241 to the

1 publisher 282. The publisher 282 decrypts  $E_{p_{KR}}[RGM]$  5241 using decryption process  
2  $D_{p_{KR}}$  and the operations center's public key  $PKR$ . The publisher 282 then encrypts the  
3 electronic book content  $EBC$ , along with the randomly generated message  $RGM$  received  
4 from the operations center 250 using encryption process  $E_{p_{KS}}$  and the publisher's private  
5 key  $p_{KS}$  and sends the resulting  $E_{p_{KS}}[EBC, RGM]$  5242 to the operations center 250. The  
6 operations center 250 decrypts  $E_{p_{KS}}[EBC, RGM]$  5242 using decryption process  $DPKS$   
7 and the publisher's public key  $PKS$ . If the randomly generated message  $RGM$  received  
8 from the publisher 282 coincides with the randomly generated message  $RGM$  that the  
9 operations center 250 originally sent to the publisher 282, the publisher's identity is  
10 verified.

11 In another embodiment, the ISO one-way authentication protocol framework, as  
12 defined in ISO standard X.509 is used to provide authentication of the publisher's  
13 identity.

14 The operations center 250 may initiate the transaction with the publisher 282 by  
15 requesting that an electronic book be delivered from the publisher 282 to the operations  
16 center 250. To validate the identity of the operations center 250, the publisher 282 and  
17 operations center 250 may use any of the above authentication method embodiments. In  
18 one embodiment, the Digital Signature Algorithm (DSA) is used, as described in U.S.  
19 Patent 5,231,668 to Kravitz, and hereby incorporated by reference.

20 In another embodiment, the operations center 250 uses a password as an identifier.  
21 This password is delivered along with the electronic book request to authenticate the  
22 operations center 250. The publisher 282 compares this password with the password the  
23 publisher 282 has for the operations center 250. If the passwords match, the source of  
24 the electronic book request, i.e., the operations center 250, is verified.

25 In yet another embodiment, public key encryption is used as a digital signature to  
26 authenticate the operations center 250. The operations center 250 encrypts the electronic  
27 book request using the operations center private key  $p_{KR}$  and send the encrypted request  
28 to the publisher 282. When the publisher 282 correctly decrypts the encrypted request



1 with the operations center's public key PKR, the identity of the operations center 250 is  
2 authenticated since only the operations center 250 has access to the operations center's  
3 private key pKR used to encrypt the electronic book request.

4 In another embodiment, depicted in Figure 28, upon initiation of the transaction,  
5 the operations center 250, serving as the recipient 4999, notifies the publisher 282,  
6 serving as the sender 4998, of the operations center's intention to request electronic book  
7 content from the publisher 282. This notification may be in the form of initial request  
8 message 5250. The publisher 282 then encrypts a randomly generated message RGM  
9 generated by the publisher 282 using encryption process  $E_{pKS}$  and the publisher's private  
10 key pKS and sends the resulting  $E_{pKS}[RGM]$  5251 to the operations center 250. The  
11 operations center 250 decrypts  $E_{pKS}[RGM]$  5251 using decryption process  $D_{pKS}$  and the  
12 publisher's public key PKS. The operations center 250 then encrypts the electronic book  
13 request EBR, along with the randomly generated message RGM received from the  
14 publisher 282 using encryption process  $E_{pKR}$  and the operations center's private key pKR,  
15 and sends the resulting  $E_{pKR}[EBR, RGM]$  5252 to the publisher 282. The publisher 282  
16 decrypts  $E_{pKR}[EBR, RGM]$  5252 using decryption process  $D_{pKR}$  and the operations center's  
17 public key PKR. If the randomly generated message RGM received from the operations  
18 center 250 coincides with the randomly generated message RGM that the publisher 282  
19 originally sent to the operations center 250, the operations center's identity is verified.

20 In another embodiment, the ISO one-way authentication protocol framework, as  
21 defined in ISO standard X.509 is used to provide authentication of the publisher's  
22 identity.

23 In yet another embodiment involving delivery of electronic book content from the  
24 publisher 282 to the operations center 250, the operations center 250 requests an  
25 electronic book from the publisher 282. The publisher 282 first authenticates the  
26 requesting operations center 250. An embodiment of the authentication sequence is  
27 shown in Figure 29, where the publisher 282 is serving as the sender 4998 and the  
28 operations center 250 is serving as the recipient 4999. To authenticate the operations

center 250 requesting an electronic book from the publisher 282, an authentication sequence may be initiated by the operations center 250. The authentication sequence begins with the operations center 250 sending a request 5290 to the publisher 282 for a given electronic book content file 5300. The publisher 282 then responds to the operations center 250 by generating and returning an authentication string 5291 to the operations center 250. The operations center 250 returns a message to the publisher 282 that contains: 1) a book identifier 5292, identifying the requested electronic book; 2) the signed authentication string 5293 that has been signed using a one-way hash function and then encrypted using the private key of the operations center 250; and 3) operations center 250 certification information 5294 that the publisher 282 can authenticate with the certificate authority 4997 (not shown in Figure 29).

Figure 30 presents the remaining steps of a secure delivery process, where the publisher 282 serves as the sender 4998 and the operations center 250 serves as the recipient 4999. First, the publisher 282 authenticates the operations center 250, shown as authentication step 5309. The publisher 282 then creates the requested electronic book file 5300 in file creation step 5310, creates an unprotected metadata header 5301 containing non-secure information about the electronic book in step 5311, and creates a protected metadata header 5302 containing secure information about the electronic book, shown in metadata header step 5312. Secure information about the electronic book may include an electronic book identifier, an identifier of the format being used for the protected metadata header 5302, the content decryption key 5306 and decryption algorithm to be used to decrypt the electronic book content, the number of copies of the electronic book that are allowed to be derived from the original electronic book version, distribution features supported for the electronic book, fair use features associated with the electronic book, and integrity checking information to ensure the protected metadata header 5302 is unaltered since its creation.

Distribution features may include the ability to sell one or more copies of the electronic book at a cost, distribute one or more copies of the electronic book at no cost,

1 or loan one or more copies of the electronic book. Fair use features may include the  
2 ability to use the electronic book for a defined time period, the ability to loan or print a  
3 number of copies of the entire electronic book or portions of the electronic book, and the  
4 ability to define and track the number of copies already loaned or printed. The publisher  
5 282 may then compress the electronic book file 5300, shown in compression step 5313,  
6 and the publisher 282 may then perform an encryption process on the electronic book file  
7 5300, shown in encryption step 5314.

8 Alternatively, the publisher 282 may perform the encryption process on the  
9 electronic book file 5300 and then compress the encrypted electronic book file. To  
10 encrypt the electronic book, the publisher 282 may use a pre-defined or randomly  
11 generated symmetric key or the publisher 282 may use its own private key. The content  
12 decryption key 5306 may then be placed in the protected metadata header 5302, shown  
13 in decryption key loading step 5315.

14 The publisher 282 then may calculate and place integrity checking information  
15 in the protected metadata header 5302, as shown in integrity checking steps 5316 and  
16 5317, respectively. Integrity checking information may include the results of a one-way  
17 hashing algorithm 5304, for example, using an algorithm as presented in Applied  
18 Cryptography by Bruce Schneier, performed on all or a portion of the protected metadata  
19 header 5302. The hashing function 5304 may be performed using the content decryption  
20 key 5306 or another predefined hashing key, resulting in hashing value 5305. The  
21 publisher 282 may then encrypt the entire protected metadata header 5302 or some  
22 portion of the protected metadata header 5302 using the public key of the operations  
23 center 250 or a pre-determined symmetric key known by both the publisher 282 and the  
24 operations center 250, as shown in encryption step 5318.

25 The packaged electronic book with metadata headers may then be delivered to the  
26 operations center 250 or the operations center 250 may retrieve the packaged electronic  
27 book from the publisher 282, as shown in delivery step 5319. Upon receipt of the  
28 packaged electronic book, along with metadata headers 5301 and 5302, by the operations

1 center 250, the operations center 250 may decrypt the protected metadata header 5302,  
2 validate that the protected metadata header 5302 has not been altered by performing a  
3 one-way hash calculation on the protected metadata header 5302 and comparing the result  
4 to the hash value 5305 contained in the protected metadata header 5302, and re-encrypt  
5 the protected metadata header 5302 for storage. Alternatively, the operations center 250  
6 may store the received packaged electronic book directly without decrypting the protected  
7 metadata header 5302.

8 Processing and storage of the decryption and encryption keys used on the  
9 protected metadata header 5302 at the operations center 250 may be done entirely in  
10 software, entirely on a secure smart card or removable device, or some combination of  
11 the two.

12 In still another embodiment, a publisher 282, or third party electronic book  
13 formatter, converts the electronic book content and associated metadata into a deliverable  
14 format. The prepared electronic book file is then delivered to the operations center 250,  
15 for example over the Internet using a secure socket layer (SSL) protected communication  
16 link. This exchange, depicted in Figure 31, may be initiated by the operations center 250,  
17 serving as the recipient 4999, sending a request message 5330 to the publisher 282,  
18 serving as the sender 4998, to deliver the requested electronic book content 5100 to the  
19 operations center 250.

20 The request message 5330 may contain a login and password sequence that is  
21 used by the publisher 282 to initially validate the operations center 250. Alternatively,  
22 or in addition, the publisher 282 may use the specific Internet Protocol (IP) address of the  
23 operations center 250, included in the request message 5330, for validation purposes. In  
24 response, the publisher 282 may send a certificate 5331, which may include identifying  
25 information and the publisher's public key PKS, to the operations center 250. The  
26 operations center 250 verifies the certificate 5331 was issued by a trusted third party  
27 certificate authority 4997. The operations center 250 compares the information in the

1 certificate that is received from the trusted third party certificate authority 4997, including  
2 the publisher's identifying information and public key PKS.

3 The operations center 250 then notifies the publisher 282 which encryption  
4 algorithms that the operations center 250 can support using a supported algorithm  
5 message 5332. The publisher 282 selects an algorithm and notifies the operations center  
6 250 of the selection using a selected algorithm message 5333. The operations center 250  
7 generates a transaction symmetric key SKT 5334, encrypts the transaction symmetric key  
8 SKT 5334 using the public key PKS of the publisher 282 and the algorithm provided in  
9 the selected algorithm message 5333 and sends the resulting  $E_{PKS}[SKT]$  5335 to the  
10 publisher 282. The publisher 282 decrypts  $E_{PKS}[SKT]$  5335 using decryption process  
11  $D_{pKS}$  and the publisher's private key pKS. The transaction symmetric key SKT 5334 is  
12 then used to encrypt and decrypt the transaction between the publisher 282 and the  
13 operations center 250.

14 Alternatively, an exchange, as depicted in Figure 32, may be initiated by the  
15 publisher 282, serving as sender 4998, by sending a request message 5340 to the  
16 operations center 250, serving as recipient 4999, that the publisher 282 wishes to deliver  
17 electronic book content to the operations center 250.

18 The request message 5340 may contain a login and password sequence that may  
19 be used by the operations center 250 to initially validate the publisher 282. Alternatively,  
20 or in addition, the operations center 250 may use the specific IP address of the publisher  
21 282, included in the request message 5340, for validation purposes. In response, the  
22 operations center 250 sends a certificate 5341 to the publisher 282 that may include  
23 identifying information and the operations center's public key PKR.

24 The publisher 282 verifies the certificate was issued by a trusted third party  
25 certificate authority 4997 (not shown in Figure 32). The publisher 282 compares the  
26 information in the certificate 5341 that is received from the trusted third party certificate  
27 authority 4997, including operations center's identifying information and public key PKR.  
28 The publisher 282 then notifies the operations center 250 which encryption algorithms

1 the publisher 282 can support using a supported algorithms message 5342. The  
 2 operations center 250 selects an algorithm and notifies the publisher 282 of the selection  
 3 via a selected algorithm message 5434. The publisher 282 generates a transaction  
 4 symmetric key SKT 5344, encrypts the transaction symmetric key SKT 5344 using the  
 5 public key PKR of the operations center 250 and the algorithm provided in the selected  
 6 algorithm message 5343 and sends the resulting  $E_{PKR}[SKT]$  5345 to the operations center  
 7 250. The operations center 250 decrypts  $E_{PKR}[SKT]$  5345 using decryption process  $D_{pKR}$   
 8 and the operations center's private key pKR. The transaction symmetric key SKT 4344  
 9 is then used to encrypt and decrypt the transaction between the publisher 282 and the  
 10 operations center 250.

11 Once the electronic book content is received and decrypted by the operations  
 12 center 250, the operations center 250 may store the electronic book file unencrypted or  
 13 may re-encrypt the electronic book file for storage. Alternatively, the operations center  
 14 250 may also compute a hash value of the electronic book file to be used for validation  
 15 the integrity of the file when recovered from storage for delivery to a home system 258.

16 To ensure the publisher 282 that the electronic book content delivered to the  
 17 operations center 250 was received, the operations center 250, serving the recipient 4999  
 18 in Figure 33, may respond to the publisher 282, serving as the sender in Figure 33, by first  
 19 generating a reply message REP as shown in reply generation step 5260. The operations  
 20 center 250 then encrypts reply message REP in the operations center's private key pKR  
 21 using encryption process  $E_{pKR}$ , resulting in  $E_{pKR}[REP]$ , as shown in encryption step 5261.  
 22 The operations center 250 then encrypts  $E_{pKR}[REP]$  in the publisher's public key PKS  
 23 using encryption process  $E_{PKS}$ , resulting in  $E_{PKS}[E_{pKR}[REP]]$ , as shown in encryption step  
 24 5262. The operations center sends  $E_{PKS}[E_{pKR}[REP]]$  to the publisher, as shown in sending  
 25 step 5263. The publisher 282 then decrypts  $E_{PKS}[E_{pKR}[REP]]$ , using decryption process  
 26  $D_{pKS}$  and the publisher's private key pKS, resulting in  $E_{pKR}[REP]$  as shown in decryption  
 27 step 5264. The publisher 282 then decrypts the resulting  $E_{pKR}[REP]$  using decryption  
 28 process  $D_{pKR}$  and the operations center's public key PKR, as shown in decryption step

1 5265. As shown in verification step 5266, the valid reception of reply message REP by  
2 publisher 282 serves as verification of receipt of the electronic book content delivered to  
3 the operations center 250 by the publisher 282.

4 In another embodiment, the ISO two-way authentication protocol framework, as  
5 defined in ISO standard X.509 is used to provide verification of receipt of electronic book  
6 content by the operations center 250.

7 Exchanging encryption key information between the publisher 282 and the  
8 operations center 250 may be done using communication networks. Alternatively,  
9 encryption key distribution may be accomplished by storing the encryption key  
10 information on a smart card, PCMCIA card device, CD ROM, or other portable memory  
11 storage device and delivering the device to the appropriate location for retrieval and use  
12 in future encryption and decryption activities. When the key is delivered in physical  
13 form, the key may have associated with it a valid time period of use. Once this period has  
14 expired, a new key is required. Alternatively, the device may support the capability to  
15 be updated remotely via a communication network.

16 Encryption, decryption, hashing, digital signature processing, formatting,  
17 compression, key management, and other security related activities presented herein that  
18 are performed by the publisher 282 or the operations center 250 may be done in hardware  
19 using a specialized processor. In an alternate embodiment, security related activities may  
20 be done in software via a standard or secure processor. In yet another alternative, a  
21 portion of security related activities may be done in software using a standard or secure  
22 processor while the remaining portion done in hardware via a specialized processor.

23 Once electronic book content is received and decrypted by the operations center  
24 250, the operations center 250 may encrypt the electronic book content EBC with a  
25 symmetric key algorithm and store the encrypted electronic book content along with any  
26 non-encrypted content associated with the electronic book in storage memory device  
27 5270 at the operations center 250. In one embodiment, depicted in Figure 34, secure  
28 storage is done on a memory device at the driver-level, where all information stored on

1 the memory storage device 5270 is encrypted by a memory device driver prior to being  
2 stored on memory storage device 5270, as described in Applied Cryptography, by Bruce  
3 Schneier and hereby incorporated by reference. In this embodiment, any content X 5272  
4 to be stored on the memory storage device 5270, including electronic book content, is  
5 encrypted using encryption process  $E_{SK}$  5274 in memory device driver 5271 and a  
6 symmetric key SK 5276, resulting in encrypted content  $E_{SK}[X]$  5273. The encrypted  
7 content  $E_{SK}[X]$  5273 is then stored on memory storage device 5270. Upon retrieval from  
8 the memory storage device 5270, decryption process  $D_{SK}$  5275 decrypts encrypted content  
9  $E_{SK}[X]$  5273 with symmetric key SK 5276, resulting in the original content X 5272. In  
10 another embodiment, secure storage is done at the file level, also as described in Applied  
11 Cryptography, by Bruce Schneier, where each file is encrypted individually with a  
12 different symmetric key prior to storage and stored in its encrypted form on memory  
13 storage device 5270. The symmetric key SK 5276 can then be stored separate from the  
14 stored encrypted content X 5272. In one such embodiment, encryption is done in  
15 hardware using a specialized encryption processor. In an alternate embodiment,  
16 encryption is done in software using a standard or secure processor.

17 To ensure the electronic book content file has not been modified while it was  
18 stored, in one embodiment, depicted in Figure 35, the operations center 250, serving as  
19 the storage site 4996, uses a one-way hashing algorithm 5280, as presented in Applied  
20 Cryptography, by Bruce Schneier and hereby incorporated by reference, where a hashing  
21 value 5281 is calculated by the operations center 250 based on the electronic book  
22 content EBC 5100 prior to encryption process 5282. The hashing value 5281, along with  
23 encrypted content  $E_{SK}[EBC]$  5284 is then stored on memory storage device 5283. When  
24 the encrypted content  $E_{SK}[EBC]$  5284 is retrieved from storage, the operations center 250  
25 decrypts encrypted content  $E_{SK}[EBC]$  5284 using decryption process  $D_{SK}$  5285 and  
26 retrieves the stored hashing value 5281. The operations center 250 then calculates a  
27 hashing value 5281', using the hashing algorithm 5280 and the retrieved electronic book  
28 content EBC 5100. Comparator 5286 compares the hashing value 5281 to the hashing



value 5281' to determine if they coincide. If hashing value 5281 and the hashing value 5281' coincide, the integrity of the electronic book content EBC 5100 retrieved for memory storage device 5283 can be ensured.

#### B. Operations Center to Home System Security

The operations centers 250 can deliver their electronic book content to home systems 258 via a secured mechanism. In one embodiment, an asymmetric public key encryption technique is used, as described in Contemporary Cryptography, edited by Gustavus Simmons, published by IEEE Press in 1992, and hereby incorporated by reference. Public key algorithms used may include the Merkle-Hellman Knapsacks technique, as described in U.S. Patent 4,218,582, the RSA technique, as described in U.S. Patent 4,405,829, the Pohlig-Hellman technique, as described in U.S. Patent 4,424,414, the Schnorr Signatures technique, as described in U.S. Patent 4,995,082, or any other public key technique.

In this embodiment, depicted in Figure 20, the operations center 250, serving as the sender 4998, first encrypts the electronic book content EBC 5100 destined for the home system 258, serving as the recipient 4999, and using a symmetric key encryption process  $E_{SK}$  5102, using DES, PKZIP, BLOWFISH, or any other symmetric encryption algorithm, resulting in encrypted content  $E_{SK}[EBC]$  5109. The encryption process  $E_{SK}$  5102 uses a symmetric key SK 5103 either randomly generated by a key generator process 5104 or previously defined and retrieved from key storage memory 5105. Then, the operations center 250 encrypts the symmetric key SK 5103 with private key encryption process  $E_{pKS}$  5106 using the operations center's private key pKS 5107, resulting in encrypted key  $E_{pKS}[SK]$  5108. Then, the operations center 250 packages encrypted key  $E_{pKS}[SK]$  5108, encrypted content  $E_{SK}[EBC]$  5109 and non-encrypted information 5110 related to the electronic book or the exchange and delivers the package to the home system 258. Using decryption process  $D_{pKS}$  5111 and the operations center's public key PKS 5112, the home system 258 decrypts the encrypted key  $E_{pKS}[SK]$  5108

1 and uses the recovered symmetric key SK 5103 to decrypt the encrypted content  
2  $E_{SK}[EBC]$  5109 using decryption process  $D_{SK}$  5113.

3 In an alternate embodiment, depicted in Figure 21, only symmetric key encryption  
4 is used, with a certificate authority 4997. The certificate authority 4997, a trusted source,  
5 provides a symmetric key to the operations center 250, serving as the sender 4998, and  
6 to the home system 258, serving as the recipient 4999. The certificate authority 4997  
7 may be an existing commercial entity such as Entrust or Verisign or a private entity  
8 established for the sole purpose of electronic book secure distribution. The operations  
9 center 250 contacts the certificate authority 4997, sending the request 5120 for the  
10 transaction symmetric key SKT 5121 to be used during the transaction. The certificate  
11 authority 4997 either randomly generates the transaction symmetric key SKT 5121 by  
12 using the key generator process 5124 or retrieves the previously defined transaction  
13 symmetric key SKT 5121 from key storage memory 5125. The transaction symmetric  
14 key SKT 5121 is encrypted by the certificate authority 4997 using the symmetric key  
15 encryption process  $E_{SKS}$  5123 using the operations center's symmetric key SKS 5122.

16 The resulting encrypted symmetric key  $E_{SKS}[SKT]$  5126 is delivered by the  
17 certificate authority 4997 to the operations center 250. The operations center 250  
18 decrypts the encrypted symmetric key  $E_{SKS}[SKT]$  5126 using decryption process  $D_{SKS}$   
19 5127 and using the operations center's symmetric key SKS 5122 to recover the  
20 transaction symmetric key SKT 5121. The operations center 250 then uses the recovered  
21 transaction symmetric key SKT 5121 received from the certificate authority 4997 to  
22 encrypt the electronic book content EBC 5100 using encryption process  $E_{SKT}$  5128,  
23 resulting in encrypted content  $E_{SKT}[EBC]$  5129. The operations center 250 delivers the  
24 encrypted content  $E_{SKT}[EBC]$  5129 to the home system 258. The transaction symmetric  
25 key SKT 5121 is also encrypted by the certificate authority 4997 using symmetric key  
26 encryption process  $E_{SKR}$  5131 and the home system's symmetric key SKR 5130. The  
27 resulting encrypted symmetric key  $E_{SKR}[SKT]$  5132 is delivered by the certificate  
28 authority 4997 to the home system 258. The home system 258 decrypts the encrypted

1 symmetric key  $E_{SKR}[SKT]$  5132 using decryption process  $D_{SKR}$  5133 and using the home  
 2 system's symmetric key SKR 5130 to recover the transaction symmetric key SKT 5121.  
 3 The home system 258 then uses the recovered transaction symmetric key SKT 5121  
 4 received from the certificate authority 4997 to decrypt the encrypted content  $E_{SKT}[EBC]$   
 5 5129 using decryption process  $D_{SKT}$  5134, resulting in the unencrypted electronic book  
 6 content 5100.

7 In yet another embodiment, depicted in Figure 22, the operations center 250,  
 8 acting as the sender 4998, generates a transaction symmetric key SKT 5140. The  
 9 operations center 250 either randomly generates the transaction symmetric key SKT 5140  
 10 by using the key generator process 5141 or retrieves the previously defined transaction  
 11 symmetric key SKT 5140 from key storage memory 5142. The operations center 250  
 12 encrypts the electronic book content EBC 5100 using encryption process  $E_{SKT}$  5143 and  
 13 the transaction symmetric key SKT 5140, and delivers the encrypted content  $E_{SKT}[EBC]$   
 14 5144 to the home system 258, acting as the recipient 4999.

15 The operations center 250 encrypts the transaction symmetric key SKT 5140  
 16 using encryption process  $E_{SKS}$  5145 and the operations center's symmetric key SKS 5146  
 17 that the operations center 250 shares with a third party certificate authority 4997 and  
 18 delivers the encrypted transaction symmetric key  $E_{SKS}[SKT]$  5147 to the third party  
 19 certificate authority 4997. The certificate authority 4997 decrypts the encrypted  
 20 transaction symmetric key  $E_{SKS}[SKT]$  5147 using decryption process  $D_{SKS}$  5148 and the  
 21 operations center's symmetric key SKS 5146. The home system 258 may contact the  
 22 certificate authority 4997 using request 5149 to obtain the transaction symmetric key SKT  
 23 5140. Prior to the certificate authority 4997 delivering the needed transaction symmetric  
 24 key 5140 to the home system 258, the home system 258 may be required to complete a  
 25 financial transaction with the certificate authority 4997, paying for the electronic book  
 26 content first. The certificate authority 4997 then encrypts the transaction symmetric key  
 27 SKT 5140 using encryption process  $E_{SKR}$  5150 and the home system's symmetric key SKR  
 28 5151 that the certificate authority 4997 shares with the home system 258, and delivers the

1 encrypted symmetric key  $E_{SKR}[SKT]$  5152 to the home system 258. The home system  
 2 258 decrypts the encrypted symmetric key  $E_{SKR}[SKT]$  5152 using decryption process  $D_{SKR}$   
 3 5153 and the home system's symmetric key SKR 5151, and uses the recovered transaction  
 4 symmetric key SKT 5140 to decrypt the encrypted content  $E_{SKT}[EBC]$  using decryption  
 5 process  $D_{SKT}$  5154, resulting in electronic book content EBC 5100.

6 In another embodiment, depicted in Figure 23a, the operations center 250, serving  
 7 as the sender 4998, encrypts the entire transaction stream TS 5165 between the operations  
 8 center 250 and the home system 258, serving as the recipient 4999. To do so, the  
 9 operations center 250 may use the sender private key pKS 5160 and encryption process  
 10  $E_{pKS}$  5161 to encrypt the transaction stream TS 5165, resulting in encrypted transaction  
 11 stream  $E_{pKS}[TS]$  5162. In this embodiment, the home system 258 uses decryption process  
 12  $D_{pKS}$  5164 and sender public key PKS 5163 to decrypt the encrypted transaction stream  
 13  $E_{pKS}[TS]$  5162.

14 In another embodiment, depicted in Figure 23b, the operations center 250, serving  
 15 as sender 4998, may use the public key of the home system 258, serving as the recipient  
 16 4999, to encrypt the transaction stream TS 5165. To do so, the operations center 250 may  
 17 use the recipient public key PKR 5171 and encryption process  $E_{PKR}$  5170 to encrypt the  
 18 transaction stream TS 5165, resulting in encrypted transaction stream  $E_{PKR}[TS]$  5173. In  
 19 this embodiment, the home system 258 uses decryption process  $D_{pKR}$  5174 and recipient  
 20 private key pKR 5172 to decrypt the encrypted transaction stream  $E_{PKR}[TS]$  5173. In  
 21 another embodiment, depicted in Figure 23c, the operations center 250, serving as sender  
 22 4998, may use a transaction symmetric key SKT 5181 that both the operations center 250  
 23 and the home system 258 have stored in advance of the transaction to encrypt the  
 24 transaction stream TS 5165. In this embodiment, the operations center 250 uses  
 25 encryption process  $E_{SKT}$  5180 and transaction symmetric key SKT 5181 to generate  
 26 encrypted transaction stream  $E_{SKT}[TS]$  5182. The home system 258 uses decryption  
 27 process  $D_{SKT}$  5183 and transaction symmetric key SKT 5181 to decrypt encrypted  
 28 transaction stream  $E_{SKT}[TS]$  5182, resulting in transaction stream TS 5165.

1 In another embodiment, depicted in Figure 24a, the operations center 250, serving  
 2 as the sender 4998, and the home system 258, serving as the recipient 4999, initiate the  
 3 transaction by negotiating a shared key to use for the transaction, using, for example, the  
 4 Elliptic Curve Diffie-Hellman key exchange algorithm, as described in U.S. Patent  
 5 4,200,700, to generate the shared transaction symmetric key. Key negotiation  
 6 information 5190 is exchanged between key generation algorithms 5191 operated by both  
 7 the operations center 250 and the home system 258. As a result of the negotiation  
 8 process, the operations center's key generator algorithm 5191 generates the transaction  
 9 symmetric key SKT 5193 and the home system's key generator algorithm 5192 generates  
 10 the transaction symmetric key SKT 5193.

11 The operations center 250 encrypts the electronic book content EBC 5100 using  
 12 encryption process  $E_{SKT}$  5194 and the shared transaction symmetric key SKT 5193 and  
 13 delivers the resulting encrypted content  $E_{SKT}[EBC]$  5195 to the home system 258. The  
 14 home system 258 uses the shared transaction symmetric key SKT 5193 and decryption  
 15 process DSKT 5196 to decrypt the encrypted content  $E_{SKT}[EBC]$  5195.

16 In a different embodiment, depicted in Figure 24b, the operations center 250  
 17 serves as the sender 4998 and home system 258 serves as the recipient 4999. Initial key  
 18 negotiation information 5200 is exchanged between the seed key generation algorithm  
 19 5201 at the operations center 250 and the seed key generation algorithm 5202 at the home  
 20 system 258. As a result, the seed key generation algorithm 5201 at the operations center  
 21 250 and the seed key generation algorithm 5202 at the home system 258 each generate  
 22 seed key SK 5203 using, for example, the Elliptic Curve Diffie-Hellman key exchange  
 23 algorithm, as described in U.S. Patent 4,200,700. Seed key 5203 is then used by key  
 24 sequence generator 5204 at the operations center 250 site to generate the first in a  
 25 sequence of keys, transaction symmetric key  $S_{KTi}$  5206. Similarly, seed key 5203 is used  
 26 by key sequence generator 5205 at the home system 258 to generate the identical  
 27 sequence of keys, beginning with transaction symmetric key  $S_{KTi}$  5206.

1           The operations center 250 encrypts the electronic book content EBC 5100 using  
2 encryption process  $E_{SKTi}$  5207 and the shared transaction symmetric key  $S_{Kti}$  5206 and  
3 delivers the resulting encrypted content  $E_{SKTi}[EBC]$  5208 to the home system 258. The  
4 home system 258 uses the transaction symmetric key  $S_{Kti}$  5206 and decryption process  
5  $DSKTi$  5209 to decrypt the encrypted content  $E_{SKTi}[EBC]$  5206. The operations center  
6 250 key sequence generator 5204 and home system 258 key sequence generator 5205  
7 continue to generate matching transaction symmetric keys for use in encrypting each  
8 subsequent transaction between the operations center 250 and the home system 258.

9           The operations center 250 may deliver the electronic book content to multiple  
10 home systems. In one embodiment, the operations center 250 delivers the electronic  
11 book content to each home system 258 independently using one of the embodiments  
12 contained herein. In an alternative embodiment, the operations center 250 may broadcast  
13 the electronic book content to multiple home systems simultaneously.

14           In one embodiment used for broadcasting, depicted in Figure 25a, the operations  
15 center 250, serving as the sender 4998, encrypts the electronic book content EBC 5100  
16 using encryption process  $E_{SKT}$  5211 and transaction symmetric key SKT 5210, resulting  
17 in encrypted content  $E_{SKT}[EBC]$  5217. The transaction symmetric key SKT 5210 is then  
18 encrypted using public key encryption process  $E_{PKA}$  5212 and public key PKA 5213 for  
19 recipient A 4999, the first home system 258 to receive the electronic book content,  
20 resulting in encrypted key  $E_{PKA}[SKT]$  5218. The transaction symmetric key SKT 5210  
21 is then encrypted using public key encryption process  $E_{PKB}$  5212' and public key PKB  
22 5213' for recipient B 4999', the second home system 258 to receive the electronic book  
23 content, resulting in encrypted key  $E_{PKB}[SKT]$  5218'. This is repeated for each of the  
24 home systems 258 receiving the electronic book content. The encrypted content  
25  $E_{SKT}[EBC]$  5217, along with the encrypted keys 5218, 5218', and 5218'', are delivered to  
26 all the receiving home systems 258. Each home system 258 uses its own private key to  
27 decrypt the transaction symmetric key SKT 5210. For example, recipient A 4999 uses  
28 decryption process  $D_{pKA}$  5214 and private key pKA 5216 to decrypt the encrypted key

1  $E_{PKA}[SKT]$  5218, recovering the transaction symmetric key SKT 5210. Decryption  
 2 process  $D_{SKT}$  5215 is then used to decrypt encrypted content  $E_{SKT}[EBC]$  5217 using  
 3 transaction symmetric key SKT 5210.

4 In another embodiment, depicted in Figure 25b, home systems may be assigned  
 5 to predefined groups. Prior to the distribution of electronic book content EBC 5100 by  
 6 operations center 250, serving as the sender 4998, for each defined group, a group  
 7 symmetric key SKG 5220 is created and distributed by the operations center 250 to each  
 8 home system 258, serving as recipients 4999, 4999' and 4999" within the group.

9 When the operations center 250 sends electronic book content EBC 5100 to a  
 10 pre-defined group of home systems 258, the operations center 250 encrypts the electronic  
 11 book content EBC 5100 using encryption process  $E_{SKG}$  5221 and the group symmetric key  
 12 SKG 5220 pre-defined for that group and delivers the encrypted content  $E_{SKG}[EBC]$  to  
 13 all the home systems in the group. Recipients 4999, 4999', and 4999" use decryption  
 14 process  $D_{SKG}$  5223 and the group symmetric key SKG 5220 for that group to which they  
 15 are assigned to decrypt the encrypted content  $E_{SKG}[EBC]$ .

16 To ensure that the electronic book content delivered by the operations center 250  
 17 to the home system 258 was not altered in route, integrity checking algorithms may be  
 18 employed. In one embodiment, depicted in Figure 26, the operations center 250, serving  
 19 as the sender 4998, uses a one-way hashing algorithm 5231, as presented in Applied  
 20 Cryptography, by Bruce Schneier, published by John Wiley & Sons, Inc. in 1996, and  
 21 hereby incorporated by reference, where a hashing value 5232 is calculated by the  
 22 operations center 250 based on the electronic book content file 5230 as an input. This  
 23 resulting hashing value 5232, along with the actual encrypted electronic book file 5237  
 24 that has been encrypted by the operations center 250 via encryption process 5235 is  
 25 delivered to the home system 258, serving as the recipient 4999.

26 The home system 258 decrypts the encrypted electronic book file 5237 using  
 27 decryption process 5236 to recover the electronic book content file 5230'. The home  
 28 system 258 then uses the hashing algorithm 5231 with the electronic book content file

1 5230' as input to generate a hashing value 5232', which is compared to the hashing value  
2 5232 delivered with the encrypted electronic book file 5237. If the hashing value 5232'  
3 calculated by the home system 258 coincides with the hashing value 5232 delivered by  
4 the operations center 250 as determined by comparator 5233, the integrity of the  
5 electronic book content file 5230' can be ensured.

6 To identify the operations center 250 delivering the electronic book and to  
7 guarantee non-repudiation, i.e., that the operations center 250 cannot deny that the  
8 electronic book was sent, the operations center 250 and home system 258 may use an  
9 authentication method. In one embodiment, the Digital Signature Algorithm (DSA) is  
10 used, as described in U.S. Patent 5,231,668, and hereby incorporated by reference. In  
11 another embodiment, the operations center 250 uses a password as an identifier. This  
12 password may be delivered along with the electronic book content to authenticate the  
13 operations center 250. The home system 258 compares this password with the password  
14 the home system 258 has for the operations center 250. If the passwords match, the  
15 source of the electronic book content, i.e., the operations center 250, is verified.

16 In yet another embodiment, public key encryption is used as a digital signature to  
17 authenticate the operations center 250 as the sender. The operations center 250 encrypts  
18 the electronic book content using the operations center's private key pKS. When the  
19 home system 258 correctly decrypts the encrypted electronic book content with the  
20 operations center's public key PKS, the identity of the operations center 250 is  
21 authenticated since only the operations center 250 has access to the operations center's  
22 private key pKS used to encrypt the electronic book content.

23 In another embodiment, depicted in Figure 27, upon initiation of the transaction,  
24 the operations center 250, serving as the sender 4998, notifies the home system 258,  
25 serving as the recipient 4999, of the operations center's intention to deliver electronic  
26 book content to the home system 258. This notification may be in the form of delivery  
27 notification message 5240. The home system 258 then encrypts a randomly generated  
28 message RGM generated by the home system 258 using encryption process EpKR and



1 the home system's private key  $p_{KR}$  and sends the resulting  $E_{p_{KR}}[RGM]$  5241 to the  
2 operations center 250. The operations center 250 decrypts  $E_{p_{KR}}[RGM]$  5241 using  
3 decryption process  $D_{p_{KR}}$  and the home system's public key  $PKR$ . The operations center  
4 250 then encrypts the electronic book content  $EBC$ , along with the randomly generated  
5 message  $RGM$  received from the home system 258 using encryption process  $E_{p_{KS}}$  and the  
6 operations center's private key  $p_{KS}$  and sends the resulting  $E_{p_{KS}}[EBC, RGM]$  5242 to the  
7 home system 258. The home system 258 decrypts  $E_{p_{KS}}[EBC, RGM]$  5242 using  
8 decryption process  $D_{p_{KS}}$  and the operations center's public key  $PKS$ . If the randomly  
9 generated message  $RGM$  received from the operations center 250 coincides with the  
10 randomly generated message  $RGM$  that the home system 258 originally sent to the  
11 operations center 250, the operations center's identity is verified.

12 In another embodiment, the ISO one-way authentication protocol framework, as  
13 defined in ISO standard X.509 is used to provide authentication of the operations center's  
14 identity.

15 The home system 258 may initiate the transaction with the operations center 250  
16 by requesting that an electronic book be delivered from the operations center 250 to the  
17 home system 258. To validate the identity of the home system 258, the operations center  
18 250 and home system 258 may use any of the above authentication method embodiments.  
19 In one embodiment, the Digital Signature Algorithm (DSA) is used, as described in U.S.  
20 Patent 5,231,668, and hereby incorporated by reference.

21 In another embodiment, the home system 258 uses a password as an identifier.  
22 This password is delivered along with the electronic book request to authenticate the  
23 home system 258. The operations center 250, or the billing and collection system 278  
24 operating on behalf of the operations center 250, compares this password with the  
25 password it has for the home system 258. If the password matches, the source of the  
26 electronic book request, i.e., the home system 258, is verified.

27 In yet another embodiment, public key encryption is used as a digital signature to  
28 authenticate the home system 258. The home system 258 encrypts the electronic book

1 request using the home system's private key  $pKR$  and sends the encrypted request to the  
 2 operations center 250, or the billing and collection system 278 operating on behalf of the  
 3 operations center 250. When the operations center 250, or the billing and collection  
 4 system 278 operating on behalf of the operations center 250 correctly decrypts the  
 5 encrypted request with the home system's public key  $PKR$ , the identity of the home  
 6 system 258 is authenticated since only the home system 258 has access to the home  
 7 system's private key  $pKR$  used to encrypt the electronic book request.

8 In another embodiment, depicted in Figure 28, upon initiation of the transaction,  
 9 the home system 258, serving as the recipient 4999, notifies the operations center 250,  
 10 serving as the sender 4998, of the home system's intention to request electronic book  
 11 content from the operations center 250. This notification may be in the form of initial  
 12 request message 5250. The operations center 250 then encrypts a randomly generated  
 13 message  $RGM$  generated by the operations center 250 using encryption process  $E_{pKS}$  and  
 14 the operations center's private key  $pKS$  and sends the resulting  $E_{pKS}[RGM]$  5251 to the  
 15 home system 258. The home system 258 decrypts  $E_{pKS}[RGM]$  5251 using decryption  
 16 process  $DPKS$  and the operations center's public key  $PKS$ . The home system 258 then  
 17 encrypts the electronic book request  $EBR$ , along with the randomly generated message  
 18  $RGM$  received from the operations center 250 using encryption process  $E_{pKR}$  and the  
 19 home system's private key  $pKR$ , and sends the resulting  $E_{pKR}[EBR, RGM]$  5252 to the  
 20 operations center 250. The operations center 250 decrypts  $E_{pKR}[EBR, RGM]$  5252 using  
 21 decryption process  $DPKR$  and the home system's public key  $PKR$ . If the randomly  
 22 generated message  $RGM$  received from the home system 258 coincides with the  
 23 randomly generated message  $RGM$  that the operations center 250 originally sent to the  
 24 home system 258, the home system's identity is verified.

25 In another embodiment, the ISO one-way authentication protocol framework, as  
 26 defined in ISO standard X.509 is used to provide authentication of the operations center's  
 27 identity.

1 In yet another embodiment of electronic book content delivery from the  
2 operations center 250 to the home system 258, the home system 258 requests an  
3 electronic book from the operations center 250. The operations center 250 first  
4 authenticates the requesting home system 258. An embodiment of the authentication  
5 sequence is shown in Figure 29, where the operations center 250 is serving as the sender  
6 4998 and the home system 258 is serving as the recipient 4999. To authenticate a home  
7 system 258 requesting an electronic book from the operations center 250, an  
8 authentication sequence may be initiated by the home system 258. The authentication  
9 sequence begins with the home system 258 sending a request 5290 to the operations  
10 center 250 for a given electronic book content file 5300. The operations center 250 then  
11 responds to the home system 258 by generating and returning an authentication string  
12 5291 to the home system 258. The home system 258 returns a message to the operations  
13 center 250 that contains: 1) a book identifier 5292, identifying the requested electronic  
14 book; 2) the signed authentication string 5293 that has been signed using a one-way hash  
15 function and then encrypted using the private key of the home system 258; and 3) home  
16 system 258 certification information 5294 that the operations center 250 can authenticate  
17 with the certificate authority 4997 (not shown in Figure 29).

18 The operations center 250 then retrieves the requested encrypted electronic book,  
19 along with its associated unprotected metadata header 5301 and protected metadata  
20 header 5302 from storage. The operations center 250 decrypts the protected metadata  
21 header 5302 and validates that the protected metadata header 5302 has not been altered  
22 by performing a one-way hash function on the protected metadata header 5302 and  
23 comparing the result to the hash value contained in the protected metadata header 5302.  
24 If the protected metadata header 5302 was stored unencrypted, the operations center 250  
25 retrieves the encrypted electronic book, along with its associated unprotected metadata  
26 header 5301 and protected metadata header 5302 from storage and validates the protected  
27 metadata header 5302 using a one-way hashing function. The operations center 250 then  
28 modifies the fields of the unprotected metadata header 5301 and protected metadata

1 header 5302 based on the home system 258 request and the rules established by the  
2 publisher 282 and the operations center 250 for electronic book use. The operations  
3 center 250 may then encrypt the entire protected metadata header 5302 or some portion  
4 of the protected metadata header 5302 using the public key of the home system 258 or  
5 a pre-determined symmetric key known by both the operations center 250 and the home  
6 system 258. The packaged electronic book with metadata headers may then be delivered  
7 to home system 258 or the home system 258 may retrieve the packaged electronic book  
8 from the operations center 250.

9       Upon receipt of the packaged electronic book, along with metadata headers 5301  
10 and 5302, by the home system 258, the home system 258 may decrypt the protected  
11 metadata header 5302, validate that the protected metadata header 5302 has not been  
12 altered by performing a one-way hash calculation on the protected metadata header 5302  
13 and comparing the result to the hash value 5305 contained in the protected metadata  
14 header 5302, and re-encrypt the protected metadata header 5302 for storage, or store the  
15 received packaged electronic book directly without decrypting the protected metadata  
16 header 5302. When the electronic book is opened for display on the viewer 266, the  
17 viewer 266 decrypts the protected metadata header 5302 using the decryption key,  
18 recovers the content decryption key, and decrypts the electronic book content for display  
19 on the viewer. Processing and storage of the decryption and encryption keys used on the  
20 protected metadata header 5302 at the home system 258 may be done entirely via  
21 software, entirely on a secure smart card or removable device, or some combination of  
22 the two.

23       In still another embodiment, an operations center 250, or third party electronic  
24 book formatter, converts the electronic book content and associated metadata into a  
25 deliverable format. The prepared electronic book file is then delivered to the home  
26 system 258, for example over the Internet using a secure socket layer (SSL) protected  
27 communication link. This exchange, depicted in Figure 31, may be initiated by the home  
28 system 258, serving as the recipient 4999, sending a request message 5330 to the

1 operations center 250, serving as the sender 4998, to deliver the requested electronic book  
2 content 5100 to the home system 258.

3 The request message 5330 may contain a login and password sequence that is  
4 used by the operations center 250 to initially validate the home system 258.  
5 Alternatively, or in addition, the operations center 250 may use the specific Internet  
6 Protocol (IP) address of the home system 258, included in the request message 5330, for  
7 validation purposes. In response, the operations center 250 may send a certificate 5331,  
8 which may include identifying information and the operations center's public key PKS,  
9 to the home system 258. The home system 258 verifies the certificate 5331 was issued  
10 by a trusted third party certificate authority 4997. The home system 258 compares the  
11 information in the certificate that is received from the trusted third party certificate  
12 authority 4997, including the operations center's identifying information and public key  
13 PKS.

14 The home system 258 then notifies the operations center 250 which encryption  
15 algorithms that the home system 258 can support using a supported algorithm message  
16 5332. The operations center 250 selects an algorithm and notifies the home system 258  
17 of the selection using a selected algorithm message 5333. The home system 258  
18 generates a transaction symmetric key SKT 5334, encrypts the transaction symmetric key  
19 SKT 5334 using the public key PKS of the operations center 250 and the algorithm  
20 provided in the selected algorithm message 5333 and sends the resulting  $E_{PKS}[SKT]$  5335  
21 to the operations center 250. The operations center 250 decrypts  $E_{PKS}[SKT]$  5335 using  
22 decryption process  $D_{PKS}$  and the operations center's private key pKS. The transaction  
23 symmetric key SKT 5334 is then used to encrypt and decrypt the transaction between the  
24 operations center 250 and the home system 258.

25 Alternatively, an exchange, as depicted in Figure 32, may be initiated by the  
26 operations center 250, serving as the sender 4998, by sending a request message 5340 to  
27 the home system 258, serving as the recipient 4999, that the operations center 250 wishes  
28 to deliver electronic book content to the home system 258.

1           The request message 5340 may contain a login and password sequence that may  
2       be used by the home system 258 to initially validate the operations center 250.  
3       Alternatively, or in addition, the home system 258 may use the specific IP address of the  
4       operations center 250, included in the request message 5340, for validation purposes. In  
5       response, the home system 258 sends a certificate 5341 to the operations center 250 that  
6       may include identifying information and the home system's public key PKR.

7           The operations center 250 verifies the certificate was issued by a trusted third  
8       party certificate authority 4997 (not shown in Figure 32). The operations center 250  
9       compares the information in the certificate 5341 which is received from the trusted third  
10      party certificate authority 4997, including home system's identifying information and  
11      public key PKR. The operations center 250 then notifies the home system 258 which  
12      encryption algorithms the operations center 250 can support using a supported algorithms  
13      message 5342. The home system 258 selects an algorithm and notifies the operations  
14      center 250 of the selection using a selected algorithm message 5434. The operations  
15      center 250 generates a transaction symmetric key SKT 5344, encrypts the transaction  
16      symmetric key SKT 5344 using the public key PKR of the home system 258 and the  
17      algorithm provided in the selected algorithm message 5343 and sends the resulting  
18       $E_{PKR}[SKT]$  5345 to the home system 258. The home system 258 decrypts  $E_{PKR}[SKT]$   
19      5345 using decryption process  $D_{PKR}$  and the home system's private key pKR. The  
20      transaction symmetric key SKT 4344 is then used to encrypt and decrypt the transaction  
21      between the operations center 250 and the home system 258.

22           Once the electronic book content is received and decrypted by the home system  
23      258, the home system 258 may store the electronic book file unencrypted or may  
24      re-encrypt the electronic book file for storage. Alternatively, the home system 258 may  
25      also compute a hash value of the electronic book file to be used for validation the  
26      integrity of the file when recovered from storage for delivery to a home system 258.

27           In still another embodiment, depicted in Figure 36, once an electronic book is  
28      selected by the home system 258, as shown in selection step 5500 and paid for, the

operations center 250 is requested to initiate the delivery of the electronic book to the requesting home system 258. The home system 258, which may be a dedicated library 262 and viewer 266, or alternatively a personal computer serving the functions of the library system 262, along with a dedicated electronic book viewer 266, is provided with the location to obtain the requested electronic book file by the operations center 250, as shown in location step 5501. This location may be an Internet website or any other location accessible by the home system 258. The operations center 250 compresses the requested electronic book file, as shown in compression step 5502. The operations center 250 then generates a random transaction symmetric key SKT, as shown in key generation step 5503 and encrypts the compressed electronic book file using encryption process ESKT and the transaction symmetric key SKT, as shown in encryption step 5504. Non secure metadata is then appended to the compressed, encrypted electronic book file, as shown in appending step 5505. The transaction symmetric key SKT is then encrypted using the public key PKR of the requesting home system 258 and encryption process  $E_{PKR}$ , as shown in encryption step 5506. The encrypted electronic book file is then digitally signed as shown in signature step 5507, for example, using the algorithm presented in Applied Cryptography by Bruce Schneier, and the private key of the operations center 250 pKS and is placed in the location provided to the home system 258 for retrieval in distribution step 5508. The operations center 250 removes the electronic book file from the location after a fixed period if the electronic book file is not retrieved by the home system 258, as shown in removal step 5509.

The home system 258 retrieves the compressed, encrypted electronic book file from the specified location and stores the retrieved encrypted electronic book file for future viewing. Non secure metadata information is stored and used to identify and manage the encrypted electronic book files residing on the home system 259 for use by the viewer 266. The operations center 250 generates a public and private key pair PKR and pKR for the home system 258 and provides the home system 258 the generated private key pKR during an initial home system 258 registration process. During this

1 initial home system 258 registration process, the operations center 250 also provides the  
2 home system 258 with the public key of the operations center 250, PKS.

3 In another embodiment, encrypted electronic book content  $E_{SK}[EBC]$  5515 is  
4 stored in compressed and encrypted format at the operations center 250 for access by  
5 requesting home systems 258. The symmetric key SK 5510 used to encrypt the electronic  
6 book content EBC 5512 is stored in protected memory at the operations center 250. In  
7 this embodiment, a home system 258, which may consist of a library 262 and viewer 266  
8 or a standalone viewer 266, contacts the operations center 250 using any one of a number  
9 of communication means as presented in the co-pending U.S. Patent Application Serial  
10 No. 09/289,957 titled ALTERNATIVE ELECTRONIC BOOK DELIVERY SYSTEMS  
11 and incorporated herein by reference, including direct dial-in by the viewer 266 using a  
12 PSTN.

13 Access to the operations center 250 by the home system 258 may be password  
14 protected where the home system 258 presents a password to the operations center 250  
15 upon accessing the operations center 250. The password provided by the home system  
16 258 must match a password the operations center 250 is expecting from a specific home  
17 system 258 for before the operations center 250 allows for the purchase of any electronic  
18 book content. A request message 5511 is sent by the home system 258 to the operations  
19 center 250 to purchase a specific electronic book EBC 5512. In this request message  
20 5511, the home system 258 provides unique identifying information, including the home  
21 system 258 internal serial number. Once the requesting home system 258 is verified  
22 using the provided password and the identifying information provided in the request  
23 message 5511, the operations center 250 retrieves the stored symmetric key SK 5510  
24 used to encrypt the requested electronic book from protected memory and encrypts  
25 symmetric key SK 5510 using encryption process  $E_{SKS}$  5512 and shared key SKS 5513.

26 The shared key SKS 5513 is obtained from the home system 258 during an initial  
27 home system 258 registration process and is stored by the operations center 250 after this  
28 initial registration process. The encrypted electronic book content  $E_{SK}[EBC]$  5515 and



1 the encrypted key  $E_{SKS}[SK]$  5514 are then moved to a location assigned to the requesting  
2 home system 258. Any encrypted electronic book and associated encrypted key residing  
3 in the home system's assigned location can then be selected and downloaded to the  
4 requesting home system 258 at any time. Other information shared by the operations  
5 center 250 and the home system 258, including the home system 258 unique internal  
6 serial number, is used to authenticate the validity of a requesting home system 258 prior  
7 to initiating the download of encrypted electronic book content to the home system 258.  
8 The operations center 250 obtains information about the home system 258, including the  
9 shared key SKS 5513 and internal serial number during an initial home system 258  
10 registration process. Also, the operations center 250 provides the assigned location for  
11 the home system 258 to retrieve future electronic book content during this registration  
12 process.

13 Once the encrypted electronic book content  $E_{SK}[EBC]$  5515 and the encrypted key  
14  $E_{SKS}[SK]$  5514 are downloaded to a home system 258, the home system 258 uses shared  
15 key SKS 5513 and decryption process  $D_{SKS}$  to decrypt the encrypted key  $E_{SKS}[SK]$  5514  
16 to recover the symmetric key SK 5510. The encrypted electronic book content  $E_{SK}[EBC]$   
17 5515 or a portion thereof is then decrypted using the recovered symmetric key SK 5510  
18 and decryption process DSK and the resulting electronic book content EBC 5512 is then  
19 decompressed for display on the viewer 266.

20 To ensure the operations center 250 that the electronic book content delivered to  
21 the home system 258 was received, the home system 258, serving as the recipient 4999  
22 in Figure 33, may respond to the operations center 250, serving as the sender in Figure  
23 33, by first generating a reply message REP as shown in step 5260. The home system  
24 258 then encrypts reply message REP in the home system's private key pKR using  
25 encryption process  $E_{pKR}$ , resulting in  $E_{pKR}[REP]$ , as shown in step 5261. The home  
26 system 258 then encrypts  $E_{pKR}[REP]$  in the operations center's public key PKS using  
27 encryption process  $E_{PKS}$ , resulting in  $E_{PKS}[E_{pKR}[REP]]$ , as shown in step 5262. The home  
28 system 250 sends  $E_{PKS}[E_{pKR}[REP]]$  to the operations center 250, as shown in step 5263.

1 The operations center 250 then decrypts  $E_{PKS}[E_{pKR}[REP]]$ , using decryption process  $D_{PKS}$   
2 and the operations center's private key  $pKS$ , resulting in  $E_{pKR}[REP]$  as shown in step  
3 5264. The operations center 250 then decrypts the resulting  $E_{pKR}[REP]$  using decryption  
4 process  $D_{pKR}$  and the home system's public key  $PKR$ , as shown in step 5265. As shown  
5 in step 5266, the valid reception of reply message  $REP$  by operations center 250 serves  
6 as verification of receipt of the electronic book content delivered to the home system 258  
7 by the operations center 250.

8 In another embodiment, the ISO two-way authentication protocol framework, as  
9 defined in ISO standard X.509 is used to provide verification of receipt of electronic book  
10 content by the home system 258.

11 Exchanging encryption key information between the operations center 250 and  
12 home system 258 may be done using communication networks. Alternatively, encryption  
13 key distribution may be accomplished by storing the encryption key information on a  
14 smart card, PCMCIA card device, CD ROM, or other portable memory storage device  
15 and delivering the device to the appropriate location for retrieval and use in future  
16 encryption and decryption activities. When the key is delivered in physical form, the key  
17 may have associated with it a valid time period of use. Once this period has expired, a  
18 new key is required. Alternatively, the device may support the capability to be updated  
19 remotely via a communication network.

20 Encryption, decryption, hashing, digital signature processing, formatting,  
21 compression, key management, and other security related activities presented herein that  
22 are performed by the operations center 250 or the home system 258 may be done in  
23 hardware using a specialized processor. In an alternate embodiment, security related  
24 activities may be done in software using a standard or secure processor. In yet another  
25 alternative, a portion of security related activities may be done in software using a  
26 standard or secure processor while the remaining portion done in hardware via a  
27 specialized processor.

1           Once electronic book content is received and decrypted by the home system 258,  
2           the home system 258 may encrypt the electronic book content EBC 5100 with a  
3           symmetric key algorithm and may store the encrypted electronic book content along with  
4           any non-encrypted content associated with the electronic book in storage memory device  
5           5270 at the home system 258. In one embodiment, depicted in Figure 34, secure storage  
6           is done on a memory device at the driver-level, where all information stored on the  
7           memory storage device 5270 is encrypted by a memory device driver prior to being stored  
8           on memory storage device 5270, as described in Applied Cryptography, by Bruce  
9           Schneier and hereby incorporated by reference. In this embodiment, any content X 5272  
10          to be stored on the memory storage device 5270, including electronic book content, is  
11          encrypted using encryption process ESK 5274 in the memory device driver 5271 and a  
12          symmetric key SK 5276, resulting in encrypted content  $E_{SK}[X]$  5273. The encrypted  
13          content  $E_{SK}[X]$  5273 is then stored on the memory storage device 5270. Upon retrieval  
14          from memory storage device 5270, decryption process  $D_{SK}$  5275 decrypts encrypted  
15          content  $E_{SK}[X]$  5273 with symmetric key SK 5276, resulting in the original content X  
16          5272. In another embodiment, secure storage is done at the file level, also as described  
17          in Applied Cryptography, by Bruce Schneier, where each file is encrypted individually  
18          with a different symmetric key prior to storage and stored in its encrypted form on  
19          memory storage device 5270. The symmetric key SK 5276 can then be stored separate  
20          from the stored encrypted content X 5272. In one such embodiment, encryption is done  
21          in hardware using a specialized encryption processor. In an alternate embodiment,  
22          encryption is done in software using a standard or secure processor.

23          To ensure the electronic book content file has not been modified while it was  
24          stored, in one embodiment, depicted in Figure 35, the home system 258, serving as the  
25          storage site 4996, uses a one-way hashing algorithm 5280, as presented in Applied  
26          Cryptography, by Bruce Schneier and hereby incorporated by reference, where a hashing  
27          value 5281 is calculated by the home system 258 based on the electronic book content  
28          EBC 5100 prior to encryption process 5282. The hashing value 5281, along with

1 encrypted content  $E_{SK}[EBC]$  5284 is then stored on memory storage device 5283. When  
2 the encrypted content  $E_{SK}[EBC]$  5284 is retrieved from storage, the home system 258  
3 decrypts encrypted content  $E_{SK}[EBC]$  5284 using decryption process  $D_{SK}$  5285 and  
4 retrieves the stored hashing value 5281. The home system 258 then calculates a hashing  
5 value 5281', using the hashing algorithm 5280 and the retrieved electronic book content  
6 EBC 5100. Comparator 5286 compares the hashing value 5281 to the hashing value  
7 5281' to determine if they coincide. If the hashing value 5281 and the hashing value  
8 5281' coincide, the integrity of the electronic book content EBC 5100 retrieved for  
9 memory storage device 5283 can be ensured.

10 The security methods described above may also be applied to the communications  
11 between an operations center 250 or cable headend and an upgraded cable set-top  
12 converter 601 that is configured to function as a library 262.

### 13 C. Library to Viewer Security

14 In one embodiment, the home system 258 combines the library 262 and viewer  
15 266 functions into a single device. In another embodiment, the home system 258  
16 includes two separate devices, a library 262 and a viewer 266. For this two device  
17 embodiment, all security processing required with the viewer 266 may be done entirely  
18 in the viewer 266. Alternatively, all security processing required with the viewer 266  
19 may be done entirely in the library 262. When security processing between the home  
20 system 258 and the viewer 266 is done by the library 262, separate security processing  
21 may be implemented between the library 262 and the viewer 266. The library 262 can  
22 deliver electronic book content to the viewer 266 via a secured mechanism.

23 In one embodiment, an asymmetric public key encryption technique is used, as  
24 described in Contemporary Cryptography, edited by Gustavus Simmons, published by  
25 IEEE Press in 1992, and hereby incorporated by reference. Public key algorithms used  
26 may include the Merkle-Hellman Knapsacks technique, as described in U.S. Patent  
27 4,218,582, the RSA technique, as described in U.S. Patent 4,405,829, the Pohlig-Hellman

1 technique, as described in U.S. Patent 4,424,414, the Schnorr Signatures technique, as  
2 described in U.S. Patent 4,995,082, or any other public key technique.

3 In this embodiment, depicted in Figure 20, the library 262, serving as the sender  
4 4998, first encrypts the electronic book content EBC 5100 destined for the viewer 266,  
5 serving as the recipient 4999, using a symmetric key encryption process  $E_{SK}$  5102, and  
6 using DES, PKZIP, BLOWFISH, or any other symmetric encryption algorithm, resulting  
7 in encrypted content  $E_{SK}[EBC]$  5109. The encryption process  $E_{SK}$  5102 uses a symmetric  
8 key SK 5103 either randomly generated by a key generator process 5104 or previously  
9 defined and retrieved from key storage memory 5105. Then, the library 262 encrypts the  
10 symmetric key SK 5103 with private key encryption process  $E_{pKS}$  5106 using the library's  
11 private key pKS 5107, resulting in encrypted key  $E_{pKS}[SK]$  5108. Then, the library 262  
12 packages encrypted key  $E_{pKS}[SK]$  5108, encrypted content  $E_{SK}[EBC]$  5109 and  
13 non-encrypted information 5110 related to the electronic book or the exchange and  
14 delivers the package to the viewer 266. Using decryption process  $D_{pKS}$  5111 and the  
15 library's public key PKS 5112, the viewer 266 decrypts the encrypted key  $E_{pKS}[SK]$  5108  
16 and uses the recovered symmetric key SK 5103 to decrypt the encrypted content  
17  $E_{SK}[EBC]$  5109 using decryption process  $D_{SK}$  5113.

18 In another embodiment, depicted in Figure 23a, the library 262, serving as the  
19 sender 4998, encrypts the entire transaction stream TS 5165 between the library 262 and  
20 the viewer 266, serving as the recipient 499. To do so, the library 262 may use the sender  
21 private key pKS 5160 and encryption process  $E_{pKS}$  5161 to encrypt the transaction stream  
22 TS 5165, resulting in encrypted transaction stream  $E_{pKS}[TS]$  5162. In this embodiment,  
23 the viewer 266 uses decryption process  $D_{pKS}$  5164 and sender public key PKS 5163 to  
24 decrypt the encrypted transaction stream  $E_{pKS}[TS]$  5162.

25 In another embodiment, depicted in Figure 23b, the library 262, serving as the  
26 sender 4998, may use the public key of the viewer 266, serving as the recipient 4999, to  
27 encrypt the transaction stream TS 5165. To do so, the library 262 may use the recipient  
28 public key PKR 5171 and encryption process  $E_{PKR}$  5170 to encrypt the transaction stream

1 TS 5165, resulting in encrypted transaction stream  $E_{PKR}[TS]$  5173. In this embodiment,  
2 the viewer 266 uses decryption process  $D_{PKR}$  5174 and recipient private key  $pKR$  5172  
3 to decrypt the encrypted transaction stream  $E_{PKR}[TS]$  5173. In another embodiment,  
4 depicted in Figure 23c, the library 262, serving as sender 4998, may use a transaction  
5 symmetric key  $SKT$  5181 that both the library 262 and the viewer 266 have stored in  
6 advance of the transaction to encrypt the transaction stream  $TS$  5165. In this  
7 embodiment, the library 262 uses encryption process  $E_{SKT}$  5180 and transaction  
8 symmetric key  $SKT$  5181 to generate encrypted transaction stream  $E_{SKT}[TS]$  5182. The  
9 viewer 266 uses decryption process  $D_{SKT}$  5183 and transaction symmetric key  $SKT$  5181  
10 to decrypt encrypted transaction stream  $E_{SKT}[TS]$  5182, resulting in transaction stream  $TS$   
11 5165.

12 In another embodiment, depicted in Figure 24a, the library 262, serving as the  
13 sender 4998, and the viewer 266, serving as the recipient 4999, initiate the transaction by  
14 negotiating a shared key to use for the transaction, using, for example, the Elliptic Curve  
15 Diffie-Hellman key exchange algorithm, as described in U.S. Patent 4,200,700, to  
16 generate the shared transaction symmetric key. Key negotiation information 5190 is  
17 exchanged between key generation algorithms 5191 operated by both the library 262 and  
18 the viewer 266. As a result of the negotiation process, the library's key generator  
19 algorithm 5191 generates the transaction symmetric key  $SKT$  5193 and the viewer's key  
20 generator algorithm 5192 generates the transaction symmetric key  $SKT$  5193.

21 The library 262 encrypts the electronic book content  $EBC$  5100 using encryption  
22 process  $E_{SKT}$  5194 and the shared transaction symmetric key  $SKT$  5193 and delivers the  
23 resulting encrypted content  $E_{SKT}[EBC]$  5195 to the viewer 266. The viewer 266 uses the  
24 shared transaction symmetric key  $SKT$  5193 and decryption process  $D_{SKT}$  5196 to decrypt  
25 the encrypted content  $E_{SKT}[EBC]$  5195. In a different embodiment, depicted in Figure  
26 24b, the library 262 serves as the sender 4998 and viewer 266 serves as the recipient  
27 4999. Initial key negotiation information 5200 is exchanged between the seed key  
28 generation algorithm 5201 at the library 262 and the seed key generation algorithm 5202

1 at the viewer 266. As a result, the seed key generation algorithm 5201 at the library 262  
2 and the seed key generation algorithm 5202 at the viewer 266 each generate seed key SK  
3 5203 using, for example, the Elliptic Curve Diffie-Hellman key exchange algorithm, as  
4 described in U.S. Patent 4,200,700. Seed key 5203 is then used by key sequence  
5 generator 5204 at the library 262 site to generate the first in a sequence of keys,  
6 transaction symmetric key SKTi 5206.

7 Similarly, seed key 5203 is used by key sequence generator 5205 at the viewer  
8 266 to generate the identical sequence of keys, beginning with transaction symmetric key  
9  $S_{K_{Ti}}$  5206. The library 262 encrypts the electronic book content EBC 5100 using  
10 encryption process  $E_{SK_{Ti}}$  5207 and the shared transaction symmetric key  $S_{K_{Ti}}$  5206 and  
11 delivers the resulting encrypted content  $E_{SK_{Ti}}[EBC]$  5208 to the viewer 266. The viewer  
12 266 uses the transaction symmetric key  $S_{K_{Ti}}$  5206 and decryption process  $D_{SK_{Ti}}$  5209 to  
13 decrypt the encrypted content  $E_{SK_{Ti}}[EBC]$  5206. The library 262 key sequence generator  
14 5204 and viewer 266 key sequence generator 5205 continue to generate matching  
15 transaction symmetric keys for use in encrypting each subsequent transaction between the  
16 library 262 and the viewer 266.

17 To ensure that the electronic book content delivered by the library 262 to the  
18 viewer 266 was not altered in route, integrity checking algorithms may be employed. In  
19 one embodiment, depicted in Figure 26, the library 262, serving as the sender 4998, uses  
20 a one-way hashing algorithm 5231, as presented in Applied Cryptography, by Bruce  
21 Schneier, published by John Wiley & Sons, Inc. in 1996, and hereby incorporated by  
22 reference, where a hashing value 5232 is calculated by the library 262 based on the  
23 electronic book content file 5230 as an input. This resulting hashing value 5232, along  
24 with the actual encrypted electronic book file 5237 that has been encrypted by the library  
25 262 via encryption process 5235 is delivered to the viewer 266, serving as the recipient  
26 4999.

27 The viewer 266 decrypts the encrypted electronic book file 5237 using decryption  
28 process 5236 to recover the electronic book content file 5230'. The viewer 266 then uses

1 the hashing algorithm 5231 with the electronic book content file 5230' as input to  
2 generate a hashing value 5232', which is compared to the hashing value 5232 delivered  
3 with the encrypted electronic book file 5237. If the hashing value 5232' calculated by the  
4 viewer 266 coincides with the hashing value 5232 delivered by the library 262 as  
5 determined by comparator 5233, the integrity of the electronic book content file 5230' can  
6 be ensured.

7 To identify the library 262 delivering the electronic book, the library 262 and  
8 viewer 266 may use an authentication method. In one embodiment, the Digital Signature  
9 Algorithm (DSA) is used, as described in U.S. Patent 5,231,668, and hereby incorporated  
10 by reference. In another embodiment, the library 262 uses a password as an identifier.  
11 This password may be delivered along with the electronic book content to authenticate  
12 the library 262 as the sender. The viewer 266 compares this password with the password  
13 the viewer 266 has for the library 262. If the passwords match, the source of the  
14 electronic book content, i.e., the library 262, is verified.

15 In yet another embodiment, public key encryption is used as a digital signature to  
16 authenticate the library 262. The library 262 encrypts the electronic book content using  
17 the library's private key pKS. When the viewer 266 correctly decrypts the encrypted  
18 electronic book content with the library's public key PKS, the identity of the library 262  
19 is authenticated since only the library 262 has access to the library's private key pKS used  
20 to encrypt the electronic book content. In another embodiment, the ISO one-way  
21 authentication protocol framework, as defined in ISO standard X.509 is used to provide  
22 authentication of the library's identity.

23 A viewer 266 may initiate the transaction with the library 262 by requesting that  
24 an electronic book be delivered from the library 262 to the viewer 266. To validate the  
25 identity of the viewer 266, the library 262 and viewer 266 may use the above  
26 authentication method embodiments. In another embodiment, the Digital Signature  
27 Algorithm (DSA) is used, as described in U.S. Patent 5,231,668, and hereby incorporated  
28 by reference. In another embodiment, the viewer 266 uses a password as an identifier.



1 This password may be delivered along with the electronic book request to authenticate  
 2 the viewer 266. The library 262 compares this password with the password the library  
 3 unit 266 has for the viewer 266. If the passwords match, the source of the electronic  
 4 book request, i.e., the viewer 266, is verified.

5 In yet another embodiment, public key encryption is used as a digital signature to  
 6 authenticate the viewer 266. The viewer 266 encrypts the electronic book request using  
 7 the viewer 266 private key pKR and send the encrypted request to the publisher 282.  
 8 When the publisher 282 correctly decrypts the encrypted request with the viewer's public  
 9 key PKR, the identity of the viewer 266 is authenticated since only the viewer 266 has  
 10 access to the viewer's private key pKR used to encrypt the electronic book request.

11 In another embodiment, depicted in Figure 28, upon initiation of the transaction,  
 12 the viewer 266, serving as the recipient 4999, notifies the library 262, serving as the  
 13 sender 4998, of the viewer's intention to request electronic book content from the library  
 14 262. This notification is in the form of initial request message 5250. The library 262  
 15 then encrypts a randomly generated message RGM generated by the library 262 using  
 16 encryption process  $E_{pKS}$  and the library's private key pKS and sends the resulting  
 17  $E_{pKS}[RGM]$  5251 to the viewer 266. The viewer 266 decrypts  $E_{pKS}[RGM]$  5251 using  
 18 decryption process  $D_{pKS}$  and the library's public key PKS. The viewer 266 then encrypts  
 19 the electronic book request EBR, along with the randomly generated message RGM  
 20 received from the library 262 using encryption process  $E_{pKR}$  and the viewer's private key  
 21 pKR and sends the resulting  $E_{pKR}[EBR, RGM]$  5252 to the library 262. The library 262  
 22 decrypts  $E_{pKR}[EBR, RGM]$  5252 using decryption process  $D_{pKR}$  and the viewer's public  
 23 key PKR. If the randomly generated message RGM received from the viewer 266  
 24 coincides with the randomly generated message RGM that the library 262 originally sent  
 25 to the viewer 266, the viewer's identity is verified.

26 In another embodiment, the ISO one-way authentication protocol framework, as  
 27 defined in ISO standard X.509 is used to provide authentication of the library's identity.

1           In yet another embodiment, the compressed and encrypted electronic book content  
2 file  $E_{SKT}[EBC]$  is stored on the library system 262. Once the electronic book is ready to  
3 be displayed on the viewer 266, the entire compressed and encrypted electronic book file  
4  $E_{SKT}[EBC]$  is downloaded to the viewer 266 from the library system 262. The viewer 266  
5 verifies the source of the electronic book by using the public key of the viewer 266 PKS  
6 to decrypt the digital signature provided. The viewer 266 then decrypts the symmetric  
7 key using decryption process  $D_{pKR}$  and the viewer's private key pKR. The viewer 266  
8 then uses decryption process  $D_{SKT}$  and the transaction symmetric key SKT to decrypt all  
9 or a portion of the electronic book file prior to display. The viewer 266 then  
10 decompresses the electronic book file and displays a page of the electronic book on the  
11 viewer 266 display.

12           Exchanging encryption key information between the library 262 and viewer 266  
13 may be done using communication networks. Alternatively, encryption key distribution  
14 may be accomplished by storing the encryption key information on a smart card,  
15 PCMCIA card device, CD ROM, or other portable memory storage device and delivering  
16 the device to the appropriate location for retrieval and use in future encryption and  
17 decryption activities. When the key is delivered in physical form, the key may have  
18 associated with it a valid time period of use. Once this period has expired, a new key  
19 may be required. Alternatively, the device may support the capability to be updated  
20 remotely via a communication network.

21           Encryption, decryption, hashing, digital signature processing, formatting,  
22 compression, key management, and other security related activities presented herein that  
23 are performed by the library 262 or the viewer 266 may be done in hardware using a  
24 specialized processor. In an alternate embodiment, security related activities may be done  
25 in software using a standard or secure processor. In yet another alternative, a portion of  
26 security related activities may be done in software using a standard or secure processor  
27 while the remaining portion done in hardware using a specialized processor.

1           Once the electronic book content EBC 5100 is received and decrypted by the  
2 viewer 266, the viewer 266 may encrypt the electronic book content EBC 5100 with a  
3 symmetric key algorithm and store the encrypted electronic book content along with any  
4 non-encrypted content associated with the electronic book in storage memory device  
5 5270 at the viewer 266. In one embodiment, depicted in Figure 34, secure storage is done  
6 on a memory device at the driver-level, where all information stored on the memory  
7 storage device 5270 is encrypted by memory device driver prior to being stored on  
8 memory storage device 5270, as described in Applied Cryptography, by Bruce Schneier  
9 and hereby incorporated by reference. In this embodiment, any content X 5272 to be  
10 stored on the memory storage device 5270, including electronic book content, is  
11 encrypted using encryption process  $E_{SK}$  5274 in memory device driver 5271 and  
12 symmetric key SK 5276, resulting in encrypted content  $E_{SK}[X]$  5273. The resulting  
13 encrypted content  $E_{SK}[X]$  5273 is then stored on memory storage device 5270. Upon  
14 retrieval from memory storage device 5270, decryption process DSK 5275 decrypts  
15 encrypted content  $E_{SK}[X]$  5273 with symmetric key SK 5276, resulting in the original  
16 content X 5272. In another embodiment, secure storage is done at the file level, also as  
17 described in Applied Cryptography, by Bruce Schneier, where each file is encrypted  
18 individually with a different symmetric key prior to storage and stored in its encrypted  
19 form on memory storage device 5270. The symmetric key SK 5276 can then be stored  
20 separate from the stored encrypted content X 5272. In one such embodiment, encryption  
21 is done in hardware using a specialized encryption processor. In an alternate  
22 embodiment, encryption is done in software using a standard or secure processor.

23           To ensure the electronic book content file has not been modified while it was  
24 stored, in one embodiment, depicted in Figure 35, the viewer 266, serving as the storage  
25 site 4996, uses a one-way hashing algorithm 5280, as presented in Applied Cryptography,  
26 by Bruce Schneier and hereby incorporated by reference, where a hashing value 5281 is  
27 calculated by the viewer 266 based on the electronic book content EBC 5100 prior to  
28 encryption process 5282. The hashing value 5281, along with the encrypted content

1  $E_{SK}[EBC]$  5284 is then stored on the memory storage device 5283. When the encrypted  
 2 content  $E_{SK}[EBC]$  5284 is retrieved from storage, the viewer 266 decrypts encrypted  
 3 content  $E_{SK}[EBC]$  5284 using decryption process  $D_{SK}$  5285 and retrieves the stored  
 4 hashing value 5281. The viewer 266 then calculates hashing value 5281', using hashing  
 5 algorithm 5280 and the retrieved electronic book content EBC 5100. Comparator 5286  
 6 compares the hashing value 5281 to the hashing value 5281' to determine if they coincide.  
 7 If the hashing value 5281 and the hashing value 5281' coincide, the integrity of the  
 8 electronic book content EBC 5100 retrieved for memory storage device 5283 can be  
 9 ensured and the viewer 266 displays the retrieved content.

10 The security methods described above may also be applied to the communications  
 11 between an upgraded cable set-top converter 601 that is configured to function as a  
 12 library unit 262 and a viewer 266.

#### 13 D. Kiosk to Viewer Security

14 Kiosks, public libraries, schools, and bookstore systems can deliver electronic  
 15 book content to a viewer 266 or public viewer 912 using a secured mechanism. In one  
 16 embodiment, an asymmetric public key encryption technique is used, as described in  
 17 Contemporary Cryptography, edited by Gustavus Simmons, published by IEEE Press in  
 18 1992, and hereby incorporated by reference. Public key algorithms used may include the  
 19 the Merkle-Hellman Knapsacks technique, as described in U.S. Patent 4,218,582, the  
 20 RSA technique, as described in U.S. Patent 4,405,829, the Pohlig-Hellman technique, as  
 21 described in U.S. Patent 4,424,414, the Schnorr Signatures technique, as described in  
 22 U.S. Patent 4,995,082, or any other public key technique.

23 In this embodiment, depicted in Figure 20, a kiosk, serving as the sender 4998,  
 24 first encrypts the electronic book content EBC 5100 destined for the viewer 266 or the  
 25 public viewer 912 (see Figure 15), serving as the recipient 4999, using a symmetric key  
 26 encryption process  $E_{SK}$  5102, and using DES, PKZIP, BLOWFISH, or any other  
 27 symmetric encryption algorithm, resulting in encrypted content  $E_{SK}[EBC]$  5109. The  
 28 encryption process  $E_{SK}$  5102 uses a symmetric key SK 5103 either randomly generated

1 by a key generator process 5104 or previously defined and retrieved from key storage  
 2 memory 5105. Then, the kiosk encrypts the symmetric key SK 5103 with private key  
 3 encryption process  $E_{pKS}$  5106 using the kiosk's private key pKS 5107, resulting in  
 4 encrypted key  $E_{pKS}[SK]$  5108. The kiosk packages encrypted key  $E_{pKS}[SK]$  5108,  
 5 encrypted content  $E_{SK}[EBC]$  5109 and non-encrypted information 5110 related to the  
 6 electronic book or the exchange and delivers the package to the viewer 266 or public  
 7 viewer 912. Using decryption process  $D_{pKS}$  5111 and the kiosk's public key PKS 5112,  
 8 the viewer 266 or public viewer 912 decrypts the encrypted key  $E_{pKS}[SK]$  5108 and uses  
 9 the recovered symmetric key SK 5103 to decrypt the encrypted content  $E_{SK}[EBC]$  5109  
 10 using decryption process DSK 5113.

11 In an alternate embodiment, depicted in Figure 21, only symmetric key encryption  
 12 is used, using a certificate authority 4997. The certificate authority 4997, a trusted  
 13 source, provides a symmetric key to each kiosk, serving as the sender 4998, and the  
 14 viewer 266 or public viewer 912, serving as the recipient 4999. The certificate authority  
 15 4997 may be an existing commercial entity such as Entrust or Verisign or a private entity  
 16 established for the sole purpose of electronic book secure distribution. The kiosk  
 17 contacts the certificate authority 4997, sending a request 5120 for a transaction symmetric  
 18 key SKT 5121 to be used during the transaction. The certificate authority 4997 either  
 19 randomly generates the transaction symmetric key SKT 5121 by using a key generator  
 20 process 5124 or retrieves the previously defined transaction symmetric key SKT 5121  
 21 from key storage memory 5125. The transaction symmetric key SKT 5121 is encrypted  
 22 by the certificate authority 4997 using symmetric key encryption process  $E_{SKS}$  5123 and  
 23 the kiosk's symmetric key SKS 5122.

24 The resulting encrypted symmetric key  $E_{SKS}[SKT]$  5126 is delivered by the  
 25 certificate authority 4997 to the kiosk. The kiosk decrypts the encrypted symmetric key  
 26  $E_{SKS}[SKT]$  5126 using decryption process  $D_{SKS}$  5127 and using the kiosk's symmetric key  
 27 SKS 5122 to recover the transaction symmetric key SKT 5121. The kiosk then uses the  
 28 recovered transaction symmetric key SKT 5121 received from the certificate authority

4997 to encrypt the electronic book content EBC 5100 using encryption process  $E_{SKT}$  5128, resulting in encrypted content  $E_{SKT}[EBC]$  5129. The kiosk delivers the encrypted content  $E_{SKT}[EBC]$  5129 to the viewer 266 or public viewer 912. The transaction symmetric key SKT 5121 is also encrypted by the certificate authority 4997 using symmetric key encryption process  $E_{SKR}$  5131 using the viewer's symmetric key SKR 5130. The resulting encrypted symmetric key  $E_{SKR}[SKT]$  5132 is delivered by the certificate authority 4997 to the viewer 266 or public viewer 912. The viewer 266 or public viewer 912 decrypts the encrypted symmetric key  $E_{SKR}[SKT]$  5132 using decryption process DSKR 5133 and the viewer's symmetric key SKR 5130 to recover the transaction symmetric key SKT 5121. The viewer 266 or public viewer 912 then uses the recovered transaction symmetric key SKT 5121 received from the certificate authority 4997 to decrypt the encrypted content  $E_{SKT}[EBC]$  5129 using decryption process  $D_{SKT}$  5134, resulting in the unencrypted electronic book content 5100.

In yet another embodiment, depicted in Figure 22, the kiosk, acting as the sender 4998, generates a transaction symmetric key SKT 5140. The kiosk either randomly generates the transaction symmetric key SKT 5140 by using the key generator process 5141 or retrieves the previously defined transaction symmetric key SKT 5140 from key storage memory 5142. The kiosk encrypts the electronic book content EBC 5100 using encryption process  $E_{SKT}$  5143 and the transaction symmetric key SKT 5140, and delivers the encrypted content  $E_{SKT}[EBC]$  5144 to the viewer 266 or public viewer 912, acting as the recipient 4999.

The kiosk encrypts the transaction symmetric key SKT 5140 using encryption process  $E_{SKS}$  5145 and the kiosk's symmetric key SKS 5146 that the kiosk shares with a third party certificate authority 4997 and delivers the encrypted symmetric key  $E_{SKS}[SKT]$  5147 to the third party certificate authority 4997. The certificate authority 4997 decrypts the encrypted symmetric key  $E_{SKS}[SKT]$  5147 using decryption process  $D_{SKS}$  5148 and the kiosk's symmetric key SKS 5146. The viewer 266 or public viewer 912 may contact the certificate authority 4997 using the request 5149 to obtain the transaction symmetric key

5140. Prior to the certificate authority 4997 delivering the needed transaction symmetric key 5140 to the viewer 266 or public viewer 912, the viewer 266 or public viewer 912 may be required to complete a financial transaction with the certificate authority 4997, paying for the electronic book content first. The certificate authority 4997 then encrypts the transaction symmetric key SKT 5140 using encryption process  $E_{SKR}$  5150 and the viewer's symmetric key SKR 5151 that the certificate authority 4997 shares with the viewer 266 or public viewer 912, and delivers the encrypted symmetric key  $E_{SKR}[SKT]$  5152 to the viewer 266 or public viewer 912. The viewer 266 or public viewer 912 decrypts the encrypted symmetric key  $E_{SKR}[SKT]$  5152 using decryption process  $D_{SKR}$  5153 and the viewer's symmetric key SKR 5151, and uses the recovered transaction symmetric key SKT 5140 to decrypt the encrypted content  $E_{SKT}[EBC]$  using decryption process  $D_{SKT}$  5154, resulting in electronic book content EBC 5100.

In another embodiment, depicted in Figure 23a, the kiosk, serving as the sender 4998, encrypts the entire transaction stream TS 5165 between the kiosk and the viewer 266 or public viewer 912, serving as the recipient 499. To do so, the kiosk may use the sender private key pKS 5160 and encryption process  $E_{pKS}$  5161 to encrypt the transaction stream TS 5165, resulting in encrypted transaction stream  $E_{pKS}[TS]$  5162. In this embodiment, the viewer 266 or public viewer 912 uses decryption process  $D_{pKS}$  5164 and sender public key PKS 5163 to decrypt the encrypted transaction stream  $E_{pKS}[TS]$  5162.

In another embodiment, depicted in Figure 23b, the kiosk, serving as the sender 4998, may use the public key of the viewer 266 or public viewer 912, serving as the recipient 4999, to encrypt the transaction stream TS 5165. To do so, the kiosk may use the recipient public key PKR 5171 and encryption process  $E_{pKR}$  5170 to encrypt the transaction stream TS 5165, resulting in encrypted transaction stream  $E_{pKR}[TS]$  5173. In this embodiment, the viewer 266 or public viewer 912 uses decryption process  $D_{pKR}$  5174 and recipient private key pKR 5172 to decrypt the encrypted transaction stream  $E_{pKR}[TS]$  5173.

1 In another embodiment, depicted in Figure 23c, the kiosk, serving as the sender  
2 4998, may use a transaction symmetric key SKT 5181 that both the kiosk and the viewer  
3 266 or public viewer 912 have stored in advance of the transaction to encrypt the  
4 transaction stream TS 5165. In this embodiment, the kiosk uses encryption process  $E_{SKT}$   
5 5180 and transaction symmetric key SKT 5181 to generate encrypted transaction stream  
6  $E_{SKT}[TS]$  5182. The viewer 266 or public viewer 912 uses decryption process  $D_{SKT}$  5183  
7 and transaction symmetric key SKT 5181 to decrypt encrypted transaction stream  
8  $E_{SKT}[TS]$  5182, resulting in transaction stream TS 5165.

9 In another embodiment, depicted in Figure 24a, the kiosk, serving as the sender  
10 4998, and viewer 266 or public viewer 912, serving as the recipient 4999, initiate the  
11 transaction by negotiating a shared key to use for the transaction, using, for example, the  
12 Elliptic Curve Diffie-Hellman key exchange algorithm, as described in U.S. Patent  
13 4,200,700, to generate the shared transaction symmetric key. Key negotiation  
14 information 5190 is exchanged between key generation algorithms 5191 operated by both  
15 the kiosk and the viewer 266 or public viewer 912. As a result of the negotiation process,  
16 the kiosk's key generator algorithm 5191 generates the transaction symmetric key SKT  
17 5192 and the viewer's key generator algorithm 5192 generates the transaction symmetric  
18 key SKT 5193.

19 The kiosk encrypts the electronic book content EBC 5100 using encryption  
20 process  $E_{SKT}$  5194 and the shared transaction symmetric key SKT 5193 and delivers the  
21 resulting encrypted content  $E_{SKT}[EBC]$  5195 to the viewer 266 or public viewer 912. The  
22 viewer 266 or public viewer 912 uses the shared transaction symmetric key SKT 5193  
23 and decryption process  $D_{SKT}$  5196 to decrypt the encrypted content  $E_{SKT}[EBC]$  5195.

24 In a different embodiment, depicted in Figure 24b, the kiosk serves as the sender  
25 4998 and viewer 266 or public viewer 912 serves as the recipient 4999. Initial key  
26 negotiation information 5200 is exchanged between the seed key generation algorithm  
27 5201 at the kiosk and the seed key generation algorithm 5202 at the viewer 266 or public  
28 viewer 912.



1 As a result, the seed key generation algorithm 5201 at the kiosk and the seed key  
2 generation algorithm 5202 at the viewer 266 or public viewer 912 each generate seed key  
3 SK 5203 using, for example, the Elliptic Curve Diffie-Hellman key exchange algorithm,  
4 as described in U.S. Patent 4,200,700. Seed key 5203 is then used by key sequence  
5 generator 5204 at the kiosk site to generate the first in a sequence of keys, transaction  
6 symmetric key  $S_{K_{Ti}}$  5206. Similarly, seed key 5203 is used by key sequence generator  
7 5205 at the viewer 266 or public viewer 912 to generate the identical sequence of keys,  
8 beginning with transaction symmetric key  $SK_{Ti}$  5206.

9 The kiosk encrypts the electronic book content EBC 5100 using encryption  
10 process  $E_{SK_{Ti}}$  5207 and the shared transaction symmetric key  $S_{K_{Ti}}$  5206 and delivers the  
11 resulting encrypted content  $E_{SK_{Ti}}[EBC]$  5208 to the viewer 266 or public viewer 912. The  
12 viewer 266 or the public viewer 912 uses the transaction symmetric key  $S_{K_{Ti}}$  5206 and  
13 decryption process  $D_{SK_{Ti}}$  5209 to decrypt the encrypted content  $E_{SK_{Ti}}[EBC]$  5206. The  
14 kiosk key sequence generator 5204 and viewer 266 or public viewer 912 key sequence  
15 generator 5205 continue to generate matching transaction symmetric keys for use in  
16 encrypting each subsequent transaction between the kiosk and the viewer 266 or public  
17 viewer 912.

18 To ensure that the electronic book content delivered by the kiosk to the viewer  
19 266 or public viewer 912 was not altered in route, integrity checking algorithms may be  
20 employed. In one embodiment, depicted in Figure 26, the kiosk, serving as sender 4998,  
21 uses a one-way hashing algorithm 5231, as presented in Applied Cryptography, by Bruce  
22 Schneier, published by John Wiley & Sons, Inc. in 1996, and hereby incorporated by  
23 reference, where a hashing value 5232 is calculated by the kiosk based on the electronic  
24 book content file 5230 as input. This resulting hashing value 5232, along with the actual  
25 encrypted electronic book file 5237 that has been encrypted by the kiosk via encryption  
26 process 5235 is delivered to the viewer 266 or public viewer 912, serving as recipient  
27 4999.

1           The viewer 266 or public viewer 912 decrypts the encrypted electronic book file  
2     5237 using decryption process 5236 to recover the electronic book content file 5230'.  
3     The viewer 266 or public viewer 912 then uses the hashing algorithm 5231 with the  
4     electronic book content file 5230' as input to generate a hashing value 5232', which is  
5     compared to the hashing value 5232 delivered with the encrypted electronic book file  
6     5237. If the hashing value 5232' calculated by the viewer 266 or public viewer 912  
7     coincides with the hashing value 5232 delivered by the kiosk as determined by  
8     comparator 5233, the integrity of the electronic book content file 5230' can be ensured.

9           To identify the kiosk of the electronic book, the kiosk and viewer 266 or the  
10    public viewer 912 may use an authentication method. In one embodiment, the Digital  
11    Signature Algorithm (DSA) is used, as described in U.S. Patent 5,231,668, and hereby  
12    incorporated by reference.

13          In another embodiment, the kiosk uses a password as an identifier. This password  
14    is delivered along with the electronic book content to authenticate the kiosk. The viewer  
15    266 or the public viewer 912 compares this password with the password the viewer 266  
16    or the public viewer 912 has for the kiosk. If the passwords match, the source of the  
17    electronic book content, i.e., the kiosk, is verified.

18          In yet another embodiment, public key encryption is used as a digital signature to  
19    authenticate the kiosk. The kiosk encrypts the electronic book content using the kiosk's  
20    private key. When the viewer 266 or the public viewer 912 correctly decrypts the  
21    encrypted electronic book content with the kiosk's public key, the identity of the kiosk  
22    is authenticated since only the kiosk has access to the kiosk's private key used to encrypt  
23    the electronic book content.

24          In another embodiment, depicted in Figure 27, upon initiation of the transaction,  
25    the kiosk, serving as the sender 4998, notifies the viewer 266 or the public viewer 912,  
26    serving as the recipient 4999, of the kiosk's intention to deliver electronic book content  
27    to the viewer 266 or public viewer 912. This notification may be in the form of delivery  
28    notification message 5240. The viewer 266 or the public viewer 912 then encrypts a

1 randomly generated message RGM generated by the viewer 266 or the public viewer 912  
2 using encryption process  $E_{p_{KR}}$  and the viewer's private key  $p_{KR}$  and sends the resulting  
3  $E_{p_{KR}}[RGM]$  5241 to the kiosk. The kiosk decrypts  $E_{p_{KR}}[RGM]$  5241 using decryption  
4 process  $D_{p_{KR}}$  and the viewer's public key  $PKR$ . The kiosk then encrypts the electronic  
5 book content EBC 5100, along with the randomly generated message RGM received from  
6 the viewer 266 or the public viewer 912 using encryption process  $E_{p_{KS}}$  and the kiosk's  
7 private key  $p_{KS}$  and sends the resulting  $E_{p_{KS}}[EBC, RGM]$  5242 to the viewer 266 or the  
8 public viewer 912. The viewer 266 or the public viewer 912 decrypts  $E_{p_{KS}}[EBC, RGM]$   
9 5242 using decryption process  $D_{p_{KS}}$  and the kiosk's public key  $PKS$ . If the randomly  
10 generated message RGM received from the kiosk coincides with the randomly generated  
11 message RGM that the viewer 266 or public viewer 912 originally sent to the kiosk, the  
12 kiosk's identity is verified. In another embodiment, the ISO one-way authentication  
13 protocol framework, as defined in ISO standard X.509 is used to provide authentication  
14 of the kiosk's identity.

15 A viewer 266 or public viewer 912 may initiate the transaction with the kiosk by  
16 requesting that an electronic book be delivered from the kiosk to the viewer 266 or the  
17 public viewer 912. To validate the identity of the viewer 266 or the public viewer 912,  
18 the kiosk and viewer 266 or the public viewer 912 may use the above authentication  
19 method embodiments. In another embodiment, the Digital Signature Algorithm (DSA)  
20 is used, as described in U.S. Patent 5,231,668, and hereby incorporated by reference. In  
21 another embodiment, the viewer 266 or the public viewer 912 uses a password as an  
22 identifier.

23 This password is delivered along with the electronic book request to authenticate  
24 the viewer 266 or the public viewer 912. The kiosk compares this password with the  
25 password it has for the viewer 266 or the public viewer 912. If the password matches,  
26 the source of the electronic book request, i.e., the viewer 266 or the public viewer 912 is  
27 verified. In yet another embodiment, public key encryption is used as a digital signature  
28 to authenticate the viewer 266 or the public viewer 912. The viewer 266 or the public

viewer 912 encrypts the electronic book request using the viewer 266 or the public viewer 912 private key  $pKR$  and send the encrypted request to the kiosk. When the kiosk correctly decrypts the encrypted request with the viewer's public key  $PKR$ , the identity of the viewer 266 or the public viewer 912 is authenticated since only the viewer 266 or the public viewer 912 has access to the viewer's private key  $pKR$  used to encrypt the electronic book request.

In another embodiment, depicted in Figure 28, upon initiation of the transaction, the viewer 266 or the public viewer 912, serving as the recipient 4999, notifies the kiosk, serving as the sender 4998, of the viewer's intention to request electronic book content from the kiosk. This notification is in the form of initial request message 5250. The kiosk then encrypts a randomly generated message  $RGM$  generated by the kiosk using encryption process  $E_{pKS}$  and the kiosk's private key  $pKS$  and sends the resulting  $E_{pKS}[RGM]$  5251 to the viewer 266 or public viewer 912. The viewer 266 or the public viewer 912 decrypts  $E_{pKS}[RGM]$  5251 using decryption process  $D_{pKS}$  and the kiosk's public key  $PKS$ . The viewer 266 or the public viewer 912 then encrypts the electronic book request  $EBR$ , along with the randomly generated message  $RGM$  received from the kiosk using encryption process  $E_{pKR}$  and the viewer's private key  $pKR$  and sends the resulting  $E_{pKR}[EBR, RGM]$  5252 to the kiosk. The kiosk decrypts  $E_{pKR}[EBR, RGM]$  5252 using decryption process  $D_{pKR}$  and the viewer's public key  $PKR$ . If the randomly generated message  $RGM$  received from the viewer 266 or the public viewer 912 coincides with the randomly generated message  $RGM$  that the kiosk originally sent to the viewer 266 or the public viewer 912, the viewer's identity is verified.

In another embodiment, the ISO one-way authentication protocol framework, as defined in ISO standard X.509 is used to provide authentication of the kiosk's identity.

In yet another embodiment, where the kiosk is functioning as a public library, a viewer 266 or the public viewer 912 requests an electronic book to be borrowed from the kiosk. The kiosk must first authenticate the viewer 266 or the public viewer 912. An embodiment of the authentication sequence is depicted in Figure 29, where the kiosk is

1 serving as sender 4998 and the viewer 266 or the public viewer 912 is serving as recipient  
2 4999. To authenticate an viewer 266 or the public viewer 912 requesting an electronic  
3 book from the kiosk, an authentication sequence may be initiated by the viewer 266 or  
4 the public viewer 912. The authentication sequence begins with the viewer 266 or the  
5 public viewer 912 sending a request 5290 to the kiosk for a given electronic book content  
6 file 5300. The kiosk then responds to the viewer 266 or the public viewer 912 by  
7 generating and returning an authentication string 5291 to the viewer 266 or the public  
8 viewer 912.

9 The viewer 266 or the public viewer 912 returns a message to the kiosk that  
10 contains: 1) a book identifier 5292, identifying the requested electronic book; 2) the  
11 signed authentication string 5293 that has been signed using a one-way hash function and  
12 then encrypted using the private key of the viewer 266 or public viewer 912; and 3)  
13 viewer 266 or the public viewer 912 certification information 5294 that the kiosk can  
14 authenticate with a certificate authority 4997. The kiosk retrieves the encrypted electronic  
15 book, along with its associated unprotected metadata header 5301 and protected metadata  
16 header 5302 from storage. The kiosk decrypts the protected metadata header 5302 using  
17 the decryption key and validates that the protected metadata header 5302 has not been  
18 altered by performing a one-way hash function on the protected metadata header 5302  
19 and comparing the result to the hash value contained in the protected metadata header  
20 5302.

21 If the protected metadata header 5302 was stored unencrypted, the kiosk retrieves  
22 the encrypted electronic book, along with its associated unprotected metadata header  
23 5301 and protected metadata header 5302 from storage and validates the protected  
24 metadata header using a one-way hashing function. The kiosk then modifies the fields  
25 of the unprotected metadata header 5301 and protected metadata header 5302 based on  
26 the viewer 266 or the public viewer 912 request and the rules established by the kiosk and  
27 the public library for electronic book uses and the loan duration time. The kiosk may  
28 then encrypt the entire protected metadata header 5302 or some portion of the protected

1 metadata header 5302 using the public key of the viewer 266 or the public viewer 912 or  
2 a pre-determined symmetric key known by both the kiosk and the viewer 266 or the  
3 public viewer 912.

4 The packaged electronic book with metadata headers may then be delivered to  
5 viewer 266 or the public viewer 912 or the viewer 266 or the public viewer 912 may  
6 retrieve the packaged electronic book from the kiosk. Upon receipt of the packaged  
7 electronic book, along with metadata headers 5301 and 5302, by the viewer 266 or the  
8 public viewer 912, the viewer 266 or the public viewer 912 may decrypt the protected  
9 metadata header 5302, validate that the protected metadata header 5302 has not been  
10 altered by performing a one-way hash calculation on the protected metadata header 5302  
11 and comparing the result to the hash value 5305 contained in the protected metadata  
12 header 5302, and re-encrypt the protected metadata header 5302 for storage, or store the  
13 received packaged electronic book directly without decrypting the protected metadata  
14 header 5302.

15 When the electronic book is opened for display on the viewer 266 or the public  
16 viewer 912, the viewer decrypts the protected metadata header 5302 using the appropriate  
17 decryption key, recovers the content decryption key, and decrypts the electronic book  
18 content for display on the viewer. To return a borrowed electronic book to a kiosk, the  
19 viewer 266 or the public viewer 912 sends a return request to the kiosk. To authenticate  
20 a kiosk and to obtain the public key of the kiosk if not already known by the viewer 266  
21 or the public viewer 912, an authentication sequence may be initiated by the viewer 266  
22 or the public viewer 912. The authentication sequence begins with the viewer 266 or the  
23 public viewer 912 sending a request to the kiosk to return a given electronic book content  
24 file. The viewer 266 or the public viewer 912 generates and inserts an authentication  
25 string in the request sent to the kiosk. The kiosk returns a message to the viewer 266 or  
26 the public viewer 912 that contains an authentication string that has been signed using a  
27 one-way hash function and then encrypted using the private key of the kiosk. The

protected metadata header 5302 or some portion of the header may then be encrypted in the public key of the kiosk or the private key of the viewer.

Once the kiosk has been authenticated by the viewer 266 or the public viewer 912, the packaged electronic book with metadata headers may then be returned to the kiosk and deleted from the viewer. The kiosk decrypts the protected metadata header 5302, modifies the protected metadata header 5302 to reflect that the electronic book is no longer being borrowed, and stores the modified protected metadata header 5302. This return process may also be used to return an electronic book to a kiosk for a refund. Processing of and storage of the decryption and encryption keys used on the protected metadata header 5302 at the viewer 266 or the public viewer 912 may be done entirely via software, entirely on a secure smart card or removable device, or some combination of the two.

To ensure the kiosk that the electronic book content delivered to the viewer 266 or the public viewer 912 was received, the viewer 266 or the public viewer 912, serving a recipient 4999 in Figure 33 may respond to the kiosk, serving as the sender in Figure 33, by first generating a reply message REP as shown in step 5260. The viewer 266 or the public viewer 912 then encrypts reply message REP in the viewer's private key pKR using encryption process  $E_{pKR}$ , resulting in  $E_{pKR}[REP]$ , as shown in step 5261. The viewer 266 or the public viewer 912 then encrypts  $E_{pKR}[REP]$  in the kiosk's public key PKS using encryption process  $E_{PKS}$ , resulting in  $E_{PKS}[E_{pKR}[REP]]$ , as shown in step 5262. The viewer 266 or the public viewer 912 sends  $E_{PKS}[E_{pKR}[REP]]$  to the kiosk, as shown in step 5263. The kiosk then decrypts  $E_{PKS}[E_{pKR}[REP]]$ , using decryption process  $D_{PKS}$  and the kiosk's private key pKS, resulting in  $E_{pKR}[REP]$  as shown in step 5264. The kiosk then decrypts the resulting  $E_{pKR}[REP]$  using decryption process  $D_{pKR}$  and the viewer's public key PKR, as shown in step 5265. As shown in step 5266, the valid reception of reply message REP by kiosk serves as verification of receipt of the electronic book content delivered to the viewer 266 or the public viewer 912 by the kiosk.

1 In another embodiment, the ISO two-way authentication protocol framework, as  
2 defined in ISO standard X.509 is used to provide verification of receipt of electronic book  
3 content by the viewer 266 or the public viewer 912. Exchanging encryption key  
4 information between the kiosk and viewer 266 or the public viewer 912 may be done via  
5 communication networks. Alternatively, encryption key distribution may be  
6 accomplished by storing the encryption key information on a smart card, PCMCIA card  
7 device, CD ROM, or other portable memory storage device and delivering the device to  
8 the appropriate location for retrieval and use in future encryption and decryption  
9 activities. When the key is delivered in physical form, the key may have associated with  
10 it a valid time period of use. Once this period has expired, a new key is required.  
11 Alternatively, the device may support the capability to be updated remotely using a  
12 communication network.

13 Encryption, decryption, hashing, digital signature processing, formatting,  
14 compression, key management, and other security related activities presented herein that  
15 are performed by the kiosk or the viewer 266 or the public viewer 912 may be done in  
16 hardware using a specialized processor. In an alternate embodiment, security related  
17 activities may be done in software using a standard or secure processor. In yet another  
18 alternative, a portion of security related activities may be done in software using a  
19 standard or secure processor while the remaining portion done in hardware using a  
20 specialized processor.

21 Once electronic book content is received and decrypted by the viewer 266 or the  
22 public viewer 912, the viewer 266 or the public viewer 912 may encrypt the electronic  
23 book content EBC 5100 with a symmetric key algorithm and store the encrypted  
24 electronic book content along with any non-encrypted content associated with the  
25 electronic book in storage memory device 5270 at the viewer 266 or the public viewer  
26 912. In one embodiment, depicted in Figure 34, secure storage is done on a memory  
27 device at the driver-level, where all information stored on the memory storage device  
28 5270 is encrypted by memory device driver prior to being stored on memory storage



device 5270, as described in Applied Cryptography, by Bruce Schneier and hereby incorporated by reference. In this embodiment, any content X 5272 to be stored on the memory storage device 5270, including electronic book content, is encrypted using encryption process  $E_{SK}$  5274 in memory device driver 5271 and symmetric key SK 5276, resulting in encrypted content  $E_{SK}[X]$  5273. The resulting encrypted content  $E_{SK}[X]$  5273 is then stored on memory storage device 5270. Upon retrieval from memory storage device 5270, decryption process  $D_{SK}$  5275 decrypts encrypted content  $E_{SK}[X]$  5273 with symmetric key SK 5276, resulting in the original content X 5272. In another embodiment, secure storage is done at the file level, also as described in Applied Cryptography, by Bruce Schneier, where each file is encrypted individually with a different symmetric key prior to storage and stored in its encrypted form on memory storage device 5270. The symmetric key SK 5276 can then be stored separate from the stored encrypted content X 5272. In one such embodiment, encryption is done in hardware using a specialized encryption processor. In an alternate embodiment, encryption is done in software using a standard or secure processor.

To ensure the electronic book content file has not been modified while it was stored, in one embodiment, depicted in Figure 35, the viewer 266 or the public viewer 912, serving as storage site 4996, uses a one-way hashing algorithm 5280, as presented in Applied Cryptography, by Bruce Schneier and hereby incorporated by reference, where a hashing value 5281 is calculated by the viewer 266 or the public viewer 912 based on the electronic book content EBC 5100 prior to encryption process 5282. This hashing value 5281, along with the encrypted content  $E_{SK}[EBC]$  5284 is then stored on memory storage device 5283. When the encrypted content  $E_{SK}[EBC]$  5284 is retrieved from storage, the viewer 266 or the public viewer 912 decrypts encrypted content  $E_{SK}[EBC]$  5284 using decryption process  $D_{SK}$  5285 and retrieves the stored hashing value 5281. The viewer 266 or the public viewer 912 then calculates hashing value 5281', using hashing algorithm 5280 and the retrieved electronic book content EBC 5100. Comparator 5286 compares hashing value 5281 to hashing value 5281' to determine if

1 they coincide. If the hashing value 5281 and the hashing value 5281' coincide, the  
2 integrity of the electronic book content EBC 5100 retrieved for memory storage device  
3 5283 can be ensured.

4 The security methods described above may also be applied to the communications  
5 between a public library system and a viewer, between a school or school library system  
6 and a viewer, and between a bookstore system and a viewer.

7 E. Viewer to Viewer Security

8 In an embodiment where an electronic book is being lent by one viewer to  
9 another, the borrowing viewer requests an electronic book to be borrowed from the  
10 lending viewer. The lending viewer may first authenticate the borrowing viewer. An  
11 embodiment of the authentication sequence is depicted in Figure 29, where the lending  
12 viewer is serving as the sender 4998 and the viewer 266 or the public viewer 912 is  
13 serving as the recipient 4999. To authenticate a borrowing viewer requesting an  
14 electronic book from the lending viewer, an authentication sequence may be initiated by  
15 the borrowing viewer. The authentication sequence begins with the borrowing viewer  
16 sending a request 5290 to the lending viewer for a given electronic book content file  
17 5300.

18 The lending viewer then responds to the borrowing viewer by generating and  
19 returning an authentication string 5291 to the borrowing viewer. The borrowing viewer  
20 returns a message to the lending viewer that contains: 1) a book identifier 5292;  
21 identifying the requested electronic book; 2) the signed authentication string 5293 that  
22 has been signed using a one-way hash function and then encrypted using the private key  
23 of the borrowing viewer; and 3) borrowing viewer certification information 5294 that the  
24 lending viewer can authenticate with a certificate authority 4997. The lending viewer  
25 retrieves the encrypted electronic book, along with its associated unprotected metadata  
26 header 5301 and protected metadata header 5302 from storage. The lending viewer  
27 decrypts the protected metadata header 5302 using the decryption key and validates that  
28 the protected metadata header 5302 has not been altered by performing a one-way hash

1 function on the protected metadata header 5302 and comparing the result to the hash  
2 value contained in the protected metadata header 5302. If the protected metadata header  
3 5302 was stored unencrypted, the lending viewer retrieves the encrypted electronic book,  
4 along with its associated unprotected metadata header 5301 and protected metadata  
5 header 5302 from storage and validates the protected metadata header using a one-way  
6 hashing function. The lending viewer then modifies the fields of the unprotected  
7 metadata header 5301 and protected metadata header 5302 based on the borrowing  
8 viewer request and the rules established by the lending viewer and the public library for  
9 electronic book uses and the loan duration time. The lending viewer may then encrypt  
10 the entire protected metadata header 5302 or some portion of the protected metadata  
11 header 5302 using the public key of the borrowing viewer or a pre-determined symmetric  
12 key known by both the lending viewer and the borrowing viewer.

13 The packaged electronic book with metadata headers may then be delivered to  
14 borrowing viewer or the borrowing viewer may retrieve the packaged electronic book  
15 from the lending viewer. Upon receipt of the packaged electronic book, along with  
16 metadata headers 5301 and 5302, by the borrowing viewer, the borrowing viewer may  
17 decrypt the protected metadata header 5302, validate that the protected metadata header  
18 5302 has not been altered by performing a one-way hash calculation on the protected  
19 metadata header 5302 and comparing the result to the hash value 5305 contained in the  
20 protected metadata header 5302, and re-encrypt the protected metadata header 5302 for  
21 storage, or store the received packaged electronic book directly without decrypting the  
22 protected metadata header 5302. When the electronic book is opened for display on the  
23 borrowing viewer, the viewer decrypts the protected metadata header 5302 using the  
24 appropriate decryption key, recovers the content decryption key, and decrypts the  
25 electronic book content for display on the viewer. To return a borrowed electronic book  
26 to a lending viewer, the borrowing viewer sends a return request to the lending viewer.  
27 To authenticate a lending viewer and to obtain the public key of the lending viewer if not

1 already known by the borrowing viewer, an authentication sequence may be initiated by  
2 the borrowing viewer.

3 The authentication sequence begins with the borrowing viewer sending a request  
4 to the lending viewer to return a given electronic book content file. The borrowing  
5 viewer generates and inserts an authentication string in the request sent to the lending  
6 viewer. The lending viewer returns a message to the borrowing viewer that contains an  
7 authentication string that has been signed using a one-way hash function and then  
8 encrypted using the private key of the lending viewer. The protected metadata header  
9 5302 or some portion of the header may then be encrypted in the public key of the  
10 lending viewer or the private key of the viewer.

11 Once the lending viewer has been authenticated by the borrowing viewer, the  
12 packaged electronic book with metadata headers may then be returned to the lending  
13 viewer and deleted from the viewer. The lending viewer decrypts the protected metadata  
14 header 5302, modifies the protected metadata header 5302 to reflect that the electronic  
15 book is no longer being borrowed, and stores the modified protected metadata header  
16 5302. Processing of and storage of the decryption and encryption keys used on the  
17 protected metadata header 5302 at the borrowing viewer may be done entirely using  
18 software, entirely on a secure smart card or removable device, or some combination of  
19 the two.

#### 20 F. Copyright Protection

21 A number of mechanisms may be implemented in the electronic book delivery  
22 system to support copyright protection. In one embodiment, all transactions between the  
23 publisher 282 and the operations center 250, the operations center 250 and home systems  
24 258, the library 262 and the viewer 266, or a kiosk and the viewer 266 or the public  
25 viewer 912, may make use of the protocol defined in the 5C Digital Transmission  
26 Content Protection Specification, developed by Hitachi, Ltd., Intel Corporation,  
27 Matsushita Electric Industrial Co., Ltd., Sony Corporation, and Toshiba Corporation,  
28 available from the Digital Transmission Licensing Administrator, at [www.dtcp.com](http://www.dtcp.com) and

hereby incorporated by reference. Alternate embodiments to support copyright protection in the distribution of electronic books are addressed below.

Visible copyright notifications may be applied to electronic book content, establishing the rights holder's legal claim to copyright protection. Copyright holder information, electronic book source information, and/or copyright disclaimer information may be embedded as a visible watermark within the electronic book. This copyright information may be associated with the electronic book and delivered with the electronic book when the electronic book is distributed from one entity to another or the electronic book is copied. The copyright information may be displayed the first time an electronic book is viewed. The copyright information may be displayed initially, each time an electronic book is viewed. Alternatively, the information may always be displayed whenever an electronic book is being viewed. This copyright information may be inserted as actual text, overlaid on electronic book text, or inserted as background graphical information in the electronic book.

Associated with a delivered electronic book may be an indication of an electronic book's printing rights. Printing rights information may be applied to all users of an electronic book title, or printing rights may apply to a specific user of an electronic book. Printing rights information may be delivered with an electronic book by the operations center 250 and used by the home system 258 in determining what printing capabilities are allowed. An electronic book may be allowed to be printed an unlimited number of times. An electronic book may be allowed to be printed one time only. An electronic book may not be allowed to be printed at all.

Finally, an electronic book may be allowed to be printed, but the electronic version of the electronic book title may be deleted after this one printing. If the electronic book viewer 266 or library 262 has a printing capability, the copyright information may be applied to the printed content. The copyright information may be applied on the first page printed, on several pages printed, or on all pages printed. The software running on the secure processor in the home system 258 performs the print management function.

1           The electronic book distribution system can make use of steganography to further  
2 protect electronic books from copyright violation attempts. Steganography serves to hide  
3 secret messages in other messages, concealing the existence of the secret message. The  
4 most familiar form of steganographic technique is invisible ink. Steganographic  
5 techniques can allow for hidden identifiers to be inserted into electronic books for  
6 identifying and tracking purposes.

7           In one embodiment, the source and various intermediate handlers of electronic  
8 book content can insert their identifying marker within an electronic book. This identifier  
9 may be a message signed with the private key of the entity inserting the identifier. In  
10 another embodiment, an identification value representing the purchasing viewer 266 or  
11 the public viewer 912 may be inserted in the electronic book using steganographic  
12 techniques. The operations center 250 may insert the purchasing viewer's identifier, or  
13 alternatively, the home system 258 may insert the purchasing viewer's identifier. In one  
14 embodiment, the steganographic technique of modifying graphics on a pixel basis is used  
15 to encode hidden identifying information. In another embodiment, non-obvious markings  
16 are added to the text of an electronic book. In yet another embodiment, modification of  
17 line spacings is used to encode hidden identifying information.

18           Audio watermarking techniques can be used to encode identifying information  
19 into audio provided with electronic books. Graphic watermarking, using HighWater  
20 Designs' fingerprinted binary information technique or Digimarc Corporation's DigiMarc  
21 technology, as defined in U.S. Patent 5,721,788, Method and System for Digital Image  
22 Signature, to Powell, hereby incorporated by reference, may be used. In yet another  
23 embodiment, video watermarking techniques may be used to encode identifying  
24 information into video provided with electronic books.

25           Prior to the delivery of the electronic book containing steganographic identifiers,  
26 a hashing value may be calculated and also delivered with the electronic book. The  
27 hashing value may be recalculated and compared with the hashing value calculated prior

1 to delivery of the electronic book to the home system 258. If the hashing values match,  
2 the steganographic identifiers can be assured to be unaltered.

3         Steganographics may be incorporated into a security and validation system.  
4 Embedded steganographic information, including the electronic book publisher 282,  
5 rightholders, the originating operations center 250, and other intermediate sources and  
6 the purchasing home system 258 identifier, may be delivered within each electronic book  
7 sold to a home system 258. Whenever a home system 258 requests the purchase of a new  
8 electronic book, the operations center 250 or billing and collection subsystem 278 may  
9 query the home system 258 to determine the sources of all resident electronic books and  
10 to ensure that the books are assigned to that specific home system 258. This query may  
11 include the operations center 250 or billing and collection subsystem 278 accessing and  
12 retrieving the steganographically-hidden information from within each electronic book  
13 stored at the home system 258. If the home system 258 contains an electronic book from  
14 a source that is not valid or an electronic book for which the home system 258 was not  
15 the valid recipient, the operations center 250 or billing and collection subsystem 278 may  
16 not allow the transaction to proceed and may send a disable command that disables the  
17 home system 258 from operation until the issue can be resolved with the operations  
18 center 250. Alternatively, the home system 258, under the control of the secure  
19 processor, may only display electronic books that are watermarked with that home  
20 system's unique identifier.

21         Critical to the security of electronic book distribution system is the ability to  
22 modify the security algorithms in case of a security breach.

23         In one embodiment, the security algorithms operating on the electronic book  
24 home system 258 are updated by software downloaded using a communication network.  
25 In an alternative embodiment, the security algorithms operating on the electronic book  
26 home system 258 are updated using software downloaded from a smart card, PC-MCIA  
27 device, or other memory device attached to the home system 258.